CLIFFORD

CHANCE

A GUIDE TO TECHNOLOGY DISPUTES IN ASIA PACIFIC

2ND EDITION (2023)

CONTENTS

INTRODUCTION

Technology impacts on every area of business in every sector. It is integral to the management and operation of a company and its systems, processes and data; delivering products and services; and engaging with customers and creating new business models. The emergence of technologies including blockchain, big data, artificial intelligence (AI) and quantum computing have opened up further opportunities. But this increasing reliance on technology and the novel legal questions raised by new technologies can give rise to complex disputes across multiple jurisdictions. In 2022, we saw an increasing number of tech disputes in the Asia Pacific (APAC) region focusing on cryptoassets, data breaches and the use of AI. We expect this trend to continue in 2023.

In this Guide, we will explore the issues that give rise to tech legal disputes, including the following:

- Protection and enforcement of technology-related rights – such as intellectual property (IP) rights in technologies and databases, and rights to exploit and monetise data – remain fundamental for the survival of companies across sectors. Attention is focused on the application of established legal principles in relation to evolving technologies, such as views on authorship, inventorship and liability in relation to AI, issues of control and recourse in relation to smart contracts, and the concepts of property and ownership when applied to digital assets and virtual worlds. Disputes testing these issues can also face challenges in obtaining and enforcing court remedies; for example, where assets are intangible, or the operation of an algorithm is difficult to explain or predict.

- As new and evolving technologies are being pioneered across a range of sectors, they continue to raise novel questions concerning the conduct of product liability claims. Failure to adequately address the risks and responsibilities arising from technology use gives rise to contractual disputes in relation to supplier contracts, investment agreements and collaboration documents.

- Shifting economic conditions and geopolitical tensions are expected to generate further disputes as bankruptcies, financial distress and collateral events disrupt certain markets – including, notably, cryptoasset markets – which can, in combination with resource and component shortages and distribution network bottlenecks, place some technology supply chains under strain.

- Antitrust authorities are continuing to focus on regulation of the digital sphere and of technology giants, with associated investigations and litigation increasing as prominent companies come under scrutiny for alleged anti-competitive behaviour connected with their use of technology and data.

- Companies are also navigating issues raised by an increasingly complex regulatory landscape in relation to technology and data. Data breaches, data misuse and the illegal transfer of personal data remain key litigation and enforcement risks due to a global proliferation of heavy-hitting data governance laws, international data flows being more challenging than ever before, and increasingly strict cybersecurity standards in many parts of the world. Technology investments and transactions, as well as launches or expansions of technology-focused companies, face increasing numbers of hurdles to overcome, including in relation to sanctions, money laundering, export controls, investment controls, licensing requirements and other restrictions. New regulatory frameworks are being established in relation to digital services and new technologies such as digital assets, with associated claims, disputes and regulatory enforcement action expected to follow as contractual rights and obligations are affected and company compliance programmes struggle to keep pace with developments in this area.

Developing a litigation strategy

When a dispute arises, consideration needs to be given to the available legal remedies and causes of action, the availability of rapid interim relief and the types of evidence that need to be gathered, in order to prevail at trial or to arrive at the optimal negotiated settlement. Such considerations should inform any litigation strategy in a technology-related dispute and influence the implementation of an overall digitalisation strategy.

In addition, large-scale technology-related litigation has become increasingly international. Disputes are frequently litigated in multiple forums, thereby increasing the complexity of such litigation. Technology companies must be prepared to litigate anywhere in the world. Commercial activity in virtual worlds adds another layer of jurisdictional complexity and will raise novel practical considerations if litigation and arbitration proceedings begin to be conducted in the metaverse or forays into “on-chain arbitration” occur.

As a consequence, litigation and arbitration strategy increasingly requires a combination of international disputes management expertise with legal specialisation in technology and data.

About this Guide

This Guide sets out some key issues arising from technology protection, regulation and disputes in Asia-Pacific. Each section features a summary of the key issues and provides guidance on how companies operating in each of the jurisdictions highlighted should best protect and enforce their IP in a digital environment, protect their data and data privacy and handle cybersecurity incidents, and deal with a range of technology regulation and disputes, such as in the areas of AML, sanctions, anti-trust, fintech, responsible tech and product / contractual liability.

The Guide covers technological issues in five key jurisdictions: (1) Hong Kong, (2) China, (3) Singapore, (4) Japan and (5) Australia. It is based on contributions from Clifford Chance's regional network in Asia Pacific.[1]

"We are seeing more disputes and litigation arising around new technologies, including in relation to AI and digital assets. Enhanced regulatory frameworks are being implemented that impact everything from data use, to cyber security, to product liability, to the resilience of the digital asset ecosystem. In this increasingly complex regulatory framework, legal issues arising in one sphere can no longer be looked at in isolation and their interplay with the rest of the legal landscape needs to be comprehensively assessed when driving an effective tech risk management strategy or navigating a technology-related dispute."

Ling Ho, Partner

1 This Guide does not purport to be comprehensive or constitute any legal advice. It is only a guide. The information and the laws referred to are correct as of August 2022 (unless otherwise stated). If you would like advice or further information on anything contained in this Guide, please contact Clifford Chance.

GLOSSARY OF TERMS AND ABBREVIATIONS

Acronym	Term
Legal and Tech	
2FA	Two factor authentication
5G	5th generation of cellular or mobile networks or communications
ADR	Alternative dispute resolution
AML	Anti-money laundering
AI	Artificial intelligence
API	Application programming interface
CAE	Cryptoasset exchange
CBDC	Central bank digital currency
CDD	Customer due diligence
CIIO	Critical information infrastructure operator (PRC)
CIO	Chief information officer
CMIC	Chinese military industrial complex
COP26	26th Conference of the Parties held in Glasgow in November 2021 and attended by signatories to United Nations Framework Convention on Climate Change
CSP	Cybersecurity service provider
CTF	Counter-terrorist financing
DAO	Decentralised autonomous organisation
DeFi	Decentralised finance
DLT	Distributed ledger technology
DPO	Data protection officer
EDSP	Electronic data storage provider
ESG	Environmental, social and governance
EV	Electric vehicle
FI	Financial institution
Fintech	Financial technology
FRAND	Fair, reasonable and non-discriminatory
ICO	Initial coin offering
ICT	Information and communications technology
IoT	Internet of Things
Infratech	Infrastructure technology
IP	Intellectual property
IP address	Internet protocol address
ISP	Internet service provider

Acronym	Term
KYC	Know your client
LEI	Legal entity identifier
NFT	Non-fungible token
NPC	Non-player character
P2P	Peer-to-peer
PEP	Politically exposed person
QR code	Quick response code
R&D	Research and development
Regtech	Regulatory technology
RIFC	Regulatory investigations and financial crime
SEO	Search engine optimisation
SEP	Standard essential patent
STO	Security token offering
SVF	Stored-value facility
UEL	Unreliable entity list (PRC)
UGC	User-generated content
VASP	Virtual asset service provider
Organisations	
ACICA	Australian Centre for International Commercial Arbitration
ACCC	Australian Competition and Consumer Commission
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
AUSTRAC	Australian Transaction Reports and Analysis Centre
CBIRC	China Banking and Insurance Regulatory Commission
CCCS	Competition and Consumer Commission of Singapore
CFIUS	Committee on Foreign Investment in the United States
CIETAC	China International Economic and Trade Arbitration Commission
CAC	Cyberspace Administration of China
CAD	Commercial Affairs Department of the Singapore Police Force
CSA	Cybersecurity Agency of Singapore
CSRC	China Securities Regulatory Commission
FATF	Financial Action Task Force
FSA	Financial Services Agency (Japan)
JBA	Japanese Bankers Association
JFTC	Japan Fair Trade Commission
HKAB	Hong Kong Association of Banks
HKIAC	Hong Kong International Arbitration Centre

Acronym	Term
HKMA	Hong Kong Monetary Authority
IA	Insurance Authority (Hong Kong)
ICO	Information Commissioner's Office (UK)
ICC	International Chamber of Commerce
JCAA	Japan Commercial Arbitration Association
JDA	Japan Digital Agency
MAS	Monetary Authority of Singapore
METI	Ministry of Economy, Trade and Industry (Japan)
MIAC	Ministry of Internal Affairs and Communications (Japan)
MOFCOM	Ministry of Commerce (PRC)
OAIC	Office of the Australian Information Commissioner
PoBC	People's Bank of China
PDPC	Personal Data Protection Commission (Singapore)
PIPC	Personal Information Protection Commission (Japan)
SAMR	State Administration for Market Regulation (PRC)
SEC	Securities and Exchange Commission (US)
SIAC	Singapore International Arbitration Centre
SFC	Securities and Futures Commission (Hong Kong)
WIPO	World Intellectual Property Organisation
Laws	
ACL	Australian Consumer Law as set out in Schedule 2 of the Competition and Consumer Act 2010
AFSL	Anti-Foreign Sanctions Law (PRC)
APPs	Australian Privacy Principles
APPI	Act on the Protection of Personal Information (Japan)
AUCL	Anti-unfair Competition Law (PRC)
DPP	Data Protection Principles (Hong Kong)
DSL	Data Security Law (PRC)
GDPR	General Data Protection Regulation (EU)
New York Convention	Convention on the Recognition and Enforcement of Foreign Arbitral Awards
OSCO	Organised and Serious Crimes Ordinance (Hong Kong)
PDPA	Personal Data Protection Act (Singapore)
PDPO	Personal Data (Privacy) Ordinance (Hong Kong)
PIPL	Personal Information Protection Law (PRC)
PTCP Act	Prevention of Transfer of Criminal Proceeds Act (Japan)
TIER	Regulations on Administration of Technology Import and Export (TIER) (PRC)
UNCITRAL	United Nations Commission on International Trade Law

PROTECTION OF TECHNOLOGY

1. PROTECTION OF TECHNOLOGY

Owning a piece of technology can come through its creation or acquisition. In either case, intellectual property (IP) is key to protecting your digital assets. IP arises either by way of statute law or – in the case of common law jurisdictions – under common law. Once vested in the owner, the owner is entitled to exploit the work in question freely and exclusively whilst being able to grant or refuse permission for others to copy or use the technology.

In the fast pace of change driven by the Internet of Things (IoT) and digitalisation, traditional IP laws and concepts may not always have caught up sufficiently to provide adequate protection for the various new forms of technologies and technology disrupters. The position is complicated by the convergence of multiple disparate technologies in a single device. Current IP concepts are focused on protecting the physical – devices, structures, the configuration and operation of physical systems and physical connections, and the physical outputs.

New and emerging technologies may pose fundamental new issues for the intellectual property system. The IoT presents challenges to existing IP protection strategies as there is clearly a need to develop new approaches better suited to the rapidly changing, connected-yet-disconnected network of innovations forming the IoT. The decentralised nature of Web3 and the opportunities it creates cause tensions to existing IP legal frameworks and concepts requiring law makers to consider law reforms to address some of the challenges.

Computer and communication software is growing in market size and economic value; software can be embedded in all types of products – from artificial intelligence (AI), medical devices to consumer products – to improve and manage intelligently the construction and operation of such devices. Consequently, the type and character of protection that is provided is of huge economic consequence.

1.1 What are the specific challenges involved in protecting the new forms of technology?

Protecting source code and making sure that general information about business ideas, together with all proprietary algorithms, will not be disclosed to third parties, are some of the biggest concerns for companies involved in innovation. In addition, data is produced exponentially in the digital economy and in society in general. It has become a new raw material with macroeconomic relevance. Non-personal data in particular, which are produced by machines and objects, and which do not comprise any information about people, are largely unregulated in law.

Whilst there is already legal protection in some areas (in particular, database copyright and trade secrets), uncertainties surrounding issues of ownership and the form of protection applicable to some of the more novel technologies will continue until the issues are eventually addressed by legislation or in the courts.

The way in which stakeholders resort to contractual relationships to manage ownership and user rights to copyright works and other IP assets also needs to be carefully considered, particularly in relation to technology surrounding crypto tokens and NFT.

1.2 How can digital products be protected?

Depending on the nature of the software product, what is considered intellectual property can be found in databases or embedded in source code. In the world of software development, we mostly talk about three types of intellectual property: copyright, patents and trade secrets.

1.3 What is the difference between copyright, patents, trade secrets and industrial designs, and how do these four types of IP apply to technology products?

(a) Copyright is what you need to protect the way your software solves a certain problem. Copyright does not protect the idea behind your product, but rather the way this idea is implemented in software. Copyright protection applies to source code, object code and user interfaces.

(b) Patents protect the idea behind a particular product, but not the execution of the idea in the form of source code. Patents often protect software architecture and proprietary algorithms. Another factor that companies should consider before settling on their IP protection strategy is cost. Applying for a patent is a complex and often costly process, which means that it may be prohibitive for smaller tech companies with limited budgets. Companies often find it worthwhile to seek advice from law firms that specialise in patent law to navigate all the complexities of obtaining patent protection.

(c) Trade secrets have to do with proprietary information that a software development company discovers and works with. Trade secrets do not require publication and can be maintained indefinitely until they are discovered by another company on the market. For instance, a tech start-up that develops business architecture which is optimal for its product. The business architecture will be the company's trade secret until somebody else, who is working in the same market, discovers – on their own – the exact same way to do the exact same thing.

(d) Industrial design, which refers to the features of a shape, configuration, pattern or ornament applied to an object by an industrial process. Registered design protects the external appearance of the object. Owners of registered designs can prevent others from using the design without the owner's permission, and they can exploit the design in many ways. Registration can also be used to protect an owner's market share by preventing others from copying the design.

1.4 How does copyright apply to source code, and how to protect your source code?

Protecting source code and making sure that general information about business ideas, together with all proprietary algorithms, will not be disclosed to third parties, are major concerns.

Creating source code is a creative process, which means that the result of such work can be protected by copyright law with the code constituting an original work of authorship.

There are two major aspects of protecting source code:

(a) Product owners have to ensure that the source code is their intellectual property and not that of a developer.

(b) Product owners have to ensure that all the details about the technical aspects of their product are kept confidential.

1.5 How can you acquire copyright protection for your source code?

Copyright is the only type of intellectual property protection that is acquired automatically whenever source code is written or a program is compiled.

A company may decide to release parts of a product's source code as open-source data; alternatively, they may maintain all of it as a trade secret. Either way, copyright protection can be applied to all source code generated. As a part of the copyright application process, the owner of the product is able to designate certain parts of source code as their company's trade secret, whereas other parts can be made available within open-source libraries.

1.6 How is a particular work protected as a trade secret?

Compared with the protection that can be achieved by patents, trade secrets do not require registration and do not have expiration dates. Most jurisdictions' laws impose conditions that information must meet in order to be considered a trade secret.

Generally, this means that the information must (1) be a secret, (2) have commercial value and (3) have been subject to steps being taken to keep it secret.

It is commonly perceived that the easiest way to protect your trade secrets is to sign a non-disclosure/confidentiality agreement. However, this may not be sufficient if no other steps or actions have been taken to keep the information secret by, for example, restricting access or disclosure on a need-to-know basis or marking the information as confidential. Compliance with such conditions may turn out to be more difficult in practice and more expensive than initially anticipated.

1.7 How are patents relevant to IoT products?

There is much debate as to whether software amounts to patentable subject matter under the laws of many countries. It is generally the case that software and methods of doing business are not patentable. In some countries, a program or algorithm is patentable, provided it is adequately embodied in a machine or computer-implemented invention that has a technical effect. The difficulty in an IoT environment is that the relevant innovation resides precisely in the program or algorithm, not the way it is embodied or restricted to a specified range of applications.

Patents in effect represent a market monopoly that can allow the patented technology to be practised independently of competitors. Patents are seen as providing both a period of monopoly and as a mechanism of allowing the patent owner to recover the front-end fixed costs in R&D investment. In the IoT environment, it is questionable to what extent patent protection provides value where it is hard to keep pace with the evolution of technology.

Nonetheless, patents may be used as leverage to obtain cross-licences to gain access to new or useful algorithms and procedures. For example, there is a fair amount of IP litigation in the United States concerning patents relevant to payment systems, communication protocols and methods. Early innovators who protected their systems have been able to secure market positions, demanding licensing fees for the use of their patented technologies.

1.8 What are the challenges in protecting integrated information networks?

Tools to enable access to information and data through computers and networks will continue to evolve and grow. Defining the rights to be held by the network and protecting the information in databases will encourage the development of the complex and sophisticated programs needed to assist with searching, linking and translating individual databases.

Network software is protected by copyright, trade secrets and/or patents in the same way as any other kind of software. Traditionally, companies have been concerned about protecting the software / algorithms that process data and the hardware that stores it. In Industry 4.0, however, the data itself is worthy of protection. This is because the IoT's promise is the ability to perform analytics on data collected from connected smart objects to lead to new knowledge and provide insights. The legal rights to these (big) datasets are therefore of paramount importance. The question of protection of the information stored in the database itself may prove much more difficult.

Apart from a jurisdiction's sui generis protection scheme, the protection of data and databases has traditionally been through trade secret and copyright laws. While useful, these laws have not always proved adequate to provide proper protection. It is most likely that contract law will best serve companies operating in the IoT space.

1.9 How can I best protect my technology and digital rights?

This depends on the jurisdiction, who the technology rights are being enforced against and whether the rights stem from an underlying contract.

A useful framework for determining how best to enforce technology rights is as follows:

(a) What right is sought to be protected?

i. The starting point is to determine the precise right that is sought to be protected and the relief that is ultimately desired.

ii. This helps narrow down the possible causes of action that might subsist and has a material bearing on the jurisdiction the rights are sought to be asserted in. Certain rights may not be enforceable in certain jurisdictions.

(b) Where do I want to assert the right?

i. The choice of forum may have a bearing on the type of remedies routinely available as a matter of course.

"Data is a precious thing and will last longer than the systems themselves."

Tim Berners-Lee, Inventor of the worldwide web

ii. It may also be useful to consider the attitudes that the various jurisdictions have adopted towards similar claims or claims premised on similar rights when considering where to bring an action.

(c) Who am I enforcing my right against?

i. If there is no contractual relationship between the parties, that may affect the ability to obtain certain types of relief.

ii. The presence or absence of a contractual relationship may also limit the available dispute resolution possibilities.

1.10 Are there any practical steps to be taken before technology is put to use?

Once rights are created or acquired, it is important to find solutions to manage and protect them appropriately.

(a) Records should be kept of the development process, relevant date(s) and authors.

(b) Appropriate contractual arrangements should be considered to maintain confidentiality of the rights.

(c) The means and forms of protection should be determined at an early stage. At the same time, it is important to ensure the right in question can be used and exploited without the risk of third-party claims.

i. It is important to understand what third-party rights may cover the rights created before commercial use or as soon as possible (to avoid wasted investment in developing the idea). In the case of patents and trademarks, this may involve patent (freedom to operate) and trademark searches.

ii. If there are any concerns about possible third-party conflicting rights or infringements, the level of risk and chances of removing the obstacle should be assessed, with consideration given to obtaining a licence or trying to agree on co-existence.

There should be a mechanism for controlling access to ensure that the right is not used inappropriately.

Such mechanisms include:

(a) processes for deciding who should be granted access and under what terms;

(b) the formulation and implementation of appropriate licences / permissions; and

(c) the implementation of technical measures to protect content.

1.11 The possible impact of FRAND and standards

For the IoT ecosystem to work in a truly seamless and interoperable way (such as in relation to the use of the underlying hardware technologies), it is likely that this ecosystem will need to use standardised technology. This is because it will need to connect objects from different commercial sources and allow the addition of new objects without disrupting the existing architecture or requiring an alternative structure. If, however, standardised elements of technology in the architecture are patented, this presents a problem as, without a licence from the relevant patent owner, third-party users of the technology may be found to have infringed those patents.

The attempted solution to this problem in the smartphone and telecom businesses, where the equivalent patents are referred to as standard essential patents (SEPs), has been for the various bodies who set standards to impose a condition that patent licences should be available to third parties on fair, reasonable and non-discriminatory (FRAND) terms.

Experience has shown that agreeing FRAND terms is not always straightforward. Parties cannot always agree on which terms are fair and reasonable, particularly as regards royalty rates. There is also a question under discussion in the courts of many jurisdictions as to what role the FRAND obligation plays when an SEP owner seeks to enforce an SEP against an alleged infringer. Even if the alleged infringer is willing to enter into a licence, it is up to the patent owner to make a FRAND offer and provide sufficient information to allow the alleged infringer to judge whether the licence is on FRAND terms. Further guidance is also welcome as to the impact on FRAND entitlements in circumstances where the licensee refuses to enter into good faith negotiations or is otherwise unwilling, as opposed to willing. The repercussions of courts in the UK, France and China willing to determine SEP licensing rates on a global basis and impose anti-suit injunctions on unwilling licensees complicates an already complex area of law.

With the development of the IoT, Web3 and the metaverse, networks of standardised technology will become even more widespread and issues such as those already experienced in the smartphone telecommunications sectors can be expected.

1.12 Protection of data

Data is unlike other conventional tangible goods. The concept of “ownership” fits neatly with ideas such as exclusive possession, the right to transfer and assign, and the right to destroy. Data, however, does not fit this well-defined category. Data can be used in many different ways by different people at a single time. No single stakeholder will have exclusive rights over data. Indeed, many different stakeholders will have different roles and responsibilities when it comes to the stewardship of data.

The difficulty of defining legal ownership rights in data is being played out in Europe where it is recognised that, whilst there is an established legal framework for exclusive intellectual property rights such as patents, copyright, trademarks and trade secrets, the nature and composition of “data” makes these traditional concepts difficult to apply.

Efforts to create exclusive ownership rights in electronic data began as long ago as 1996 with the Database Directive. The Directive gives full copyright protection to

original databases that arise out of creative human efforts and a limited fifteen-year *sui generis* right for non-original databases.[2] European case law has shown that substantial investment in a database is not sufficient to attract copyright protection. Whilst copyright provides a broad swathe of exclusive rights over a long time period, the requirement for originality and the territorial limitations of the exclusivity lessens the suitability of the concept in respect of data.

Again, whilst the Trade Secrets Protection Directive (2016) provides a degree of protection to data, it applies only to information "*generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question*" (Article 2.1(a)). It does not apply to data that is published online or shared, for example on community forums.

Much discussion centres on the implications of the General Data Protection Regulation (GDPR). However even here, European lawmakers have backed away from any concept of private ownership rights by data subjects in their personal data, choosing to give data subjects rights such as the right not to have their personal data processed without their consent.

The concept of "*data ownership*" becomes one of control: how can I obtain it, use it and prevent others from also using it to optimise my strategic advantage? The model for many online platforms and service providers is one of "*data exchange*", whereby, in order to receive requested content, one is asked to provide certain personal information (such as an email address) and to accept the placement of cookies, opening up possibilities for targeted advertising.

The inadequacies of traditional intellectual property concepts as they apply to data has led some to suggest that the most appropriate means of protection are contractual.

This too has difficulties in Europe, given the different jurisdictions and legal systems and the lack of harmonisation of contract law across the EU. Consideration should be given as to whether the inclusion of clauses dealing with data ownership, and concepts such as confidentiality should be included in agreements given potential issues with enforcement.

1.13 Protection of databases

Under copyright law, data is generally protected in the form of databases. The protection applies to the compilation, arrangement or selection of the content which is the result of a creative human effort; protection, however, applies to the database's structure and expression, not its content. As a result, computer-generated databases or simple databases do not qualify for copyright protection.

Some countries afford *sui generis* rights to databases. The right prohibits the extraction or reutilisation of any databases in which there has been substantial investment in obtaining, verifying or presenting the contents of the data. Most databases in the IoT are generated by software through an automated computer process without the

2 The European Directive is being reviewed as part of a proposed Data Act. The proposal for the new Data Act (published in 2022) provides that the sui generis database right introduced by the Database Directive is not applicable to databases containing data obtained from or generated by the use of a connected device.

involvement of creative human effort. The current state of laws in APAC offers little comfort or certainty that the data generated on a digital platform (such as blockchain) would be afforded I P protection.

Given the current uncertainty around legal protection of data, companies should take practical measures to manage and control their rights over data generated in their business, including:

(a) keeping records of the creation process, including the authors involved, time and place of creation, and any copies made of the data;

(b) putting in place contracts before disclosure of or access to the data, including licences, confidentiality measures and appropriate restraints of access and use, as well as recording instances of disclosure;

(c) ensuring that all use of underlying information for the creation of data is not subject to any third-party rights or disclosure or sharing requirements; and

(d) in the case of personal data, ensuring compliance with local data privacy laws.

Jurisdiction	Copyright protection	Sui generis protection	Trade secret / confidential information
Hong Kong	Yes	No	Yes
China	Yes	No	Yes
Singapore	Yes	No	Yes
Japan	Yes	No	Yes
Australia	Yes	No	Yes

1.14 Blockchain

Blockchain is the technology that underpins the digital currency Bitcoin – but it has far wider applications and is being commercialised in a growing number of areas. The term "blockchain" refers to the combination of a number of technologies, including its particular data structure (in which the data is built up in successive blocks), the use of public key cryptography (ensuring that each participant is uniquely identified and can validate any changes), distributed ledgers (in which each authorised participant (a node) maintains a complete version of the ledger) and consensus mechanisms (in which proposed changes to the blockchain are approved by the nodes having reached a consensus as to the validity of the proposed transaction).

Compared with traditional database technologies, blockchain can be relatively cheap and require considerably less IT investment to maintain. Further, blockchain is said to have the advantages of creating resilient, tamper-proof, distributed, decentralised and transparent records. Thus, blockchain has generated particular interest in the financial sector such as initiatives for bank-specific cryptocurrencies and self-executing smart contracts for simple financial contracts. Jurisdictions such as Delaware also recognise the potential for blockchain in securities clearing and have passed laws to expressly

permit an issuer to issue securities that are evidenced solely by a record on a blockchain. In addition, initiatives have been proposed in the public sector for government-maintained registries – for example, real estate title registries – as well as in the public interest / aid sector e.g., blockchain-based tracing of donations from donor to recipient.

The technology poses significant challenges to traditional legal concepts. For example:

Data: Distributed consensus technologies involve the sharing of detailed information on transactions. The shared nature of the blockchain gives rise to a range of issues around information sharing including confidentiality. The use of the same public key by a network participant for multiple transactions will make the participant identifiable. Further, hashing (assigning data with a code known as a hash) only pseudonymises, rather than anonymises, data. As network participants, their computers and persons whose data are being processed can be located anywhere in the world, and there remains the need to comply with the laws of various jurisdictions including, potentially, the GDPR in relation to personal data protection and cybersecurity. In relation to the GDPR, due to multiple network participants, difficulties arise in identifying them and their respective responsibilities as data controllers or processors.

Further, immutability, one of the key features of blockchain, seems to conflict with the principles of the right to be forgotten (data subjects may request erasure on specific grounds such as data no longer being necessary for the purpose for which it was collected) and storage limitation (data must be kept in such a way that enable data subjects to be identified for no longer than is necessary). That said, some concerns may be addressed by placing restrictions in permissioned blockchains or storing personal data off chain. There is also the question of who owns the data stored on a blockchain and whether such data may be protected by intellectual property rights.

Liability: Will the blockchain operator or the authorised participants be liable for a mistake in the execution of changes to the blockchain? Who will be responsible for ensuring that cross-border transfers of data comply with the relevant local legal and regulatory requirements? The GDPR gives a right for data subjects to request erasure of their personal data. Given the immutability of data on a blockchain and depending on how data are stored, enforcing the “right to be forgotten” may potentially present a challenge.

Antitrust: From an antitrust perspective, how much information are participants, who may be competitors, sharing with each other on the blockchain, and does the consensus mechanism have any hidden anti-competitive effects?

Jurisdictional issues: These are potentially acute in the blockchain context. Parties are commonly located in different jurisdictions and may be anonymous from one another. Smart contracts may be entered into by self-executing computer programs rather than people. A distributed network is very unlikely to exist in just one country. The location of exchanges on which cryptoassets are stored and traded, or platforms on which smart contracts are created and performed, may be more readily identifiable, but this is not always the case.

Choice of law and jurisdiction agreements have long been used to reduce these types of uncertainties. What choice to make is a complex question. Careful thought should be given to the laws that may best protect a party's interests. Regulation (or outright bans) in certain jurisdictions may undermine the process. For example, in China, cryptocurrency-related business activities are banned. The jurisdictions that will provide a fair and efficient forum for the resolution of disputes should also be considered.

As for arbitration, see our briefing **Arbitration for Cryptoassets and Smart Contract Disputes**, which discusses the advantages of arbitration, how to enter into an arbitration agreement, choosing arbitration rules and the issues surrounding "on chain" arbitration and enforcement.

1.15 Hardware Enablers and Smart Products

The IoT ecosystem consists of three elements: solutions, connectivity (hardware) and sensors. Most discussions around the IoT have focused on solutions. The underlying hardware and sensor technologies are often neglected. These hardware and sensor technologies, however, are the very ones that enable IoT applications to be linked together or connected to third-party systems.

Developing IoT hardware can be complex, involving the use of third-party parts (such as sensors), technologies (such as wireless and connectivity with different solutions), compliance with product safety certifications, and security and original design issues. The good news is that there is better clarity on the legal issues following a series of cases around handheld devices. Hardware products may experience similar disputes around patents, registered designs and copyrights.

1.16 Artificial Intelligence

Machine learning and artificial intelligence (AI), with the capacity to unlock huge volumes of data, are already being used across a wide range of sectors to cut costs; improve performance; and create new processes, services and products. AI will remain a driver for innovation across sectors, from healthcare and pharmaceuticals, to automotive, to insurance and financial services. As the transformative potential of AI-enabled technology is being realised in practice, regulatory scrutiny and consumer concern about the legal, ethical and data protection risks of using AI continue to grow. The hidden or unethical use of AI, or failure to tackle the risk of AI bias, can cause severe reputational damage to businesses. Regulatory oversight will also target the prudential aspects of "responsible AI" – companies will be expected to have in place documented governance frameworks with clear lines of accountability, and robust development, testing and monitoring processes throughout the AI life cycle, and those with oversight responsibilities will be required to have the right expertise. Businesses will also need to understand their reliance on any third-party AI. Correspondingly, as legal requirements relating to AI expand and AI use becomes more widespread and potentially more independent of human involvement, questions arise as to liability, and rights and ownership in potential copyright works and patentable inventions. IP and commercial disputes relating to AI can be expected. For further discussion, see **section 12** "Artificial Intelligence and the Internet of Things" below.

1.17 Quantum leap

Thanks to a global wave of private and public funding, quantum computing has moved from an R&D niche to a computing revolution. With significant advances in hardware, algorithms, fault tolerance and error-correction in the past decade, we are now beginning to see a developing ecosystem and value chain. Using quantum computing to complement and leverage existing technology, such as AI, cloud platforms and classical computing, we will begin to see a "quantum advantage" in a range of business use cases and solutions to high-impact problems that are currently intractable. Those monitoring the progress of quantum computing technology are anticipating advances in drug discovery and development, chemistry and finance.

Cybersecurity: Quantum computing has the potential to break much of today's cryptography, which is used for secure communications, financial payments, data protection, identity authentication and cryptocurrencies. While it may be some time before quantum computing has a practical impact on the effectiveness of our current cryptography, information that is encrypted now might be vulnerable in the future. Many organisations will now be considering moving to post-quantum encryption methods and upgrades to IT infrastructure.

Regulatory considerations: Given quantum computing's national security implications, the technology is already subject to export restrictions, notification requirements and foreign investment controls in a range of jurisdictions. We can expect further legislation as governments protect their national security interests and pursue policies of 'technological sovereignty' and, in time, requirements around governance, oversight, transparency and equitable access. Controls will be particularly important for decision-making that incorporates quantum-facilitated AI, where explainability and liability can be complex.

On the board's agenda: Across a range of sectors, many CEOs and CIOs will be allocating resources to start planning for quantum technology. Businesses will begin exploring partnerships with quantum hardware and software developers as well as academic institutions to help anticipate the need for quantum computing talent. The quantum computing sector itself will see increased investment, and M&A and listing activity, as the beginnings of commercial traction are on the horizon for what was once a theoretical technology.

For more, see our Talking Tech publications **A Quantum Leap – Recent Quantum Computing M&A and IPOs, Regulatory Responses and Preparing for a Paradigm Shift;** and **Emerging Technologies and the Rule of Law – It's Quantum**.

1.18 Into the metaverse

The metaverse is being hailed as the next generation of digital interaction and e-commerce. We have seen novel commercial forays into existing virtual worlds that are already a second home for much of Gen Z. In the future, we will see businesses exploring how to build, operate in and expand metaverse microcosms as they anticipate a future where a significant consumer population has digital identities beyond games and virtual hangouts. This will also mean that we will start to see exploration of how our laws may apply, be enforced, and evolve, in the metaverse.

The "direct-to-avatar" economy: As well as augmenting existing business models, the metaverse will provide entirely new markets. Companies will be anticipating an expansion in the provision of virtual services via a customer's online presence (such as online meetings, medical appointments, concerts and exercise classes) as well as exploring the provision of virtual goods to avatars themselves. We expect to see an increase in companies partnering with digital platforms to sell digital assets ranging from designer clothes to virtual real estate. Ahead of this, brand owners will be giving careful consideration to how to exploit and protect their intellectual property. With aspects of the building of the metaverse being based on new technology (including the application of AI), the question of potential patent protection and freedom to operate will also be important to consider.

Fintech meets Web 3.0 and the metaverse: We expect to see experimentation with technologies that can impact the development of the internet and the metaverse. Distributed ledger technology (DLT), which has underpinned a booming cryptoasset industry, may provide the building blocks for a decentralised Web 3.0 and decentralised autonomous organisations (DAOs), which will shape ownership, control and commerce. Non-fungible tokens (NFTs), currently prominent in the arts and entertainment industries, might go on to facilitate trade and investment in virtual goods, alongside cryptocurrencies that are becoming ever more mainstream.

Making connections: Technology such as 3-D scanning sensors, augmented reality glasses and audio equipment will proliferate, allowing for ever more immersive interaction. Improvements in the Internet of Things (IoT) and 5G technology will speed up data transfer, expanding possibilities for the use of virtual and augmented reality at scale. Companies will also begin to explore how to take robotics to the next level through the metaverse – for example, immersive environments enabling offshore wind farm maintenance and high-precision surgery through robot avatars – regardless of the real-world location of human expertise.

Real-world law in virtual reality: From employee monitoring to consumer analytics, the metaverse and metaverse-like microcosms represent potentially vast sources of data, some types of which will not have been meaningfully collected before. Data security, privacy, employment and consumer protection law will be high on the list of considerations for companies wishing to tap into user data, whether related to consumers or workers, particularly as data protection enjoys increasing regulatory attention globally. More broadly, businesses will need to keep everything – from antitrust laws to payments regulations to tax implications – in mind when expanding into the metaverse and interacting with the increasing number of firms seeking to collaborate in, and capitalise on, the development of virtual and augmented realities.

For more, see our Talking Tech publication **The Metaverse: What are the Legal Implications?** See also our client briefings **The Metaverse: Risks and Opportunities for Businesses** and **The Metaverse: Will it Change the World and Why Should I Care?**

1.19 NFTs on the rise

Increased investor focus on crypto has also propelled investor interest in areas of decentralised ledger technology such as non-fungible tokens (NFTs) i.e., cryptoassets representing proof of title to a unique digital version of an underlying asset. We have seen the market for NFTs grow rapidly, particularly in the sports and digital arts sectors, with NFT issuances selling out in record time and generating millions of dollars.

In terms of what's next, there will be additional use cases for NFTs beyond the creation of collectibles or art. For example, it is not hard to imagine the use of NFTs in a Web 3.0 environment. A metaverse, where users collaborate and trade virtual goods, is likely to make use of NFTs as a means of owning virtual property. The legal ramifications of this will be interesting because the regulatory frameworks being developed generally do not include metaverse assets.

We also expect to see the emergence of new financial products recognising these tokens as a new asset class. There are already proposals to use NFTs as collateral for financing transactions and we expect traditional finance providers and incumbents to begin offering such products. This will trigger novel operational and legal challenges, such as determining the appropriate security mechanism for these assets.

With such growth, there needs to be focus on consumer risks. As organisations and individuals look to NFTs as an opportunity to generate new revenue streams, there is concern that consumers may not be fully aware of the specific rights (if any) that are being acquired via the NFT. With very little regulation specifically dealing with NFTs currently in place, potential NFT issuers should be aware of reputational and mis-selling risks which could affect their brand and lead to legal challenges down the line.
For further discussion, see **section 11** "Fintech" below and our briefing **Non-Fungible Tokens: The Global Legal Impact**. See also **NFTs: An Introduction and Some Key Intellectual Property Considerations** for what is being acquired via a NFT (which does not necessarily include an assignment of copyright or other intellectual property rights in the underlying asset), as well as how brands are capitalising on NFTs and enforcement of any applicable intellectual property rights and governing terms.

1.20 Local legal considerations

(a) What is the usual term of protection for IP rights?

Jurisdiction	Patent	Copyright	Registered Design	Trade Secret
Hong Kong	Standard patents in Hong Kong, have a maximum term of protection of 20 years The maximum term of protection of a short-term patent is eight years	Generally, 50 years after the death of the author, or publication	Initial period of five years beginning on the filing date of the application up to a maximum of 25 years	Indefinitely until the information becomes public knowledge
China	Invention patents in China have a maximum term of protection of 20 years The maximum term of protection of a utility model patent is 10 years	Generally, 50 years after the death of the author, or publication	The maximum term of protection of a design patent is 15 years	Indefinitely until the information becomes public knowledge
Singapore	Patents in Singapore have a maximum term of protection of up to 20 years	Generally, 70 years after the death of the author, or publication In respect of published editions of literary, dramatic, musical and artistic works, 25 years from the end of the year in which the edition was first published In respect of broadcasts and cable programmes, 50 years from the end of the year in which the broadcast or cable programme was first made	Initial period of five years beginning on the filing date of the application (after which there may be renewal for two further five year terms) up to a maximum total of 15 years	Indefinitely until the information becomes public knowledge

Jurisdiction	Patent	Copyright	Registered Design	Trade Secret
Japan	Patent rights in Japan have a duration of 20 years from the filing date of the patent application. The duration of certain patent rights may be extended for a period of up to five years Utility model rights in Japan have a duration of 10 years from the filing date of the application	Generally, 70 years after the death of the author In the case of the copyright to work whose authorship is attributed to a corporation or other organisation, 70 years after the work is made public	The term of protection of a design right is 20 years after the date of its registration for designs filed before 1 April 2020; designs filed after this date have a term of protection of 25 years	Indefinitely, so long as the information meets the requirements of (a) trade secret or (b) data for limited provision, as described below
Australia	Standard patents in Australia have a duration of 20 years from the filing date of the patent application (or 25 years for pharmaceutical substance patents) Innovation patents have a duration of eight years from the filing date of the patent application (however, innovation patents are being phased out – the last day to file a new innovation patent was 25 August 2021)	For literary, dramatic, musical and artistic works, generally 70 years from the end of the year of the author's death or from the end of the year in which a literary work was published. For unpublished works, the copyright term may not commence until publication takes place. Audio-visual and other material may be subject to shorter terms of copyright protection	The term of registration of a design is five years, running from the issue of a Certificate of Registration for the design or, if the registration of the design is renewed, for 10 years. If registration is not renewed, then the design will pass into the public domain upon the expiry of the original five year period (and after a six month grace period) and is then free for anyone to use.	Indefinitely until the information becomes public knowledge. Trade secrets can be protected by statute, contract or by an obligation arising under the law or in equity as to breaches of confidentiality.

(b) Requirements for trade secret protection

Jurisdiction	Requirements for trade secret protection
Hong Kong	To succeed in the tort of breach of confidence, the following must be satisfied: 1. the trade secret itself must have the necessary "quality of confidence" about it, which excludes informa tion already in the public domain or that can be readily deduced from what is in the public domain (on the other hand, applying skill and labour to compile or put together publicly known materials can create a trade secret); 2. the trade secret must have been imparted in circumstances where there is an obligation of confidence; and 3. there must have been unauthorised use of the trade secret to the detriment of the party originally imparting the trade secret.
China	The PRC Anti-unfair Competition Law (AUCL) is the primary law applicable to the protection of trade secrets in China. The latest iteration of the law took effect on 23 April 2019 (2019 AUCL). The 2019 AUCL defines "trade secrets" – which is notably a gradually broadening concept as the AUCL evolves over time – as technical, operational and other commercial information not known to the public that has "commercial value" and for which measures have been taken to maintain confidentiality. The 2019 AUCL prohibits a business operator from: 1 obtaining trade secrets from rights holders by theft, bribery, fraud, intimidation, electronic intrusion or other improper means; 2. disclosing, using or allowing others to use the trade secrets of rights holders obtained through any of the means mentioned above; 3. disclosing, using or allowing others to use the trade secrets in its possession in violation of the confidentiality undertakings or the confidentiality requirements stipulated by rights holders; or 4. instigating, enticing or assisting others to obtain, disclose, use or allow others to use the trade secrets of right holders in violation of the confidentiality undertakings or the confidentiality requirements stipulated by the rights holders. The 2019 AUCL provides that, where a third party knows or ought to be aware that an employee or former employee of the rights owner of commercial secrets (or any other entity or individual) has committed any of the illegal acts listed above – but nonetheless accepts, publishes, uses or allows any others to use such secrets – the third party will itself be deemed to have infringed the trade secrets. Therefore, even though the third party may not have obtained the trade secrets directly from an employee, the third party, as long as it has actual or constructive knowledge of the unlawful disclosure / misappropriation, could still be liable if the employee or former employee disclosed the trade secrets unlawfully in the first place. Among other penalties, the fine for infringement of trade secrets under the 2019 AUCL has been significantly increased and now ranges from a minimum of CNY100,000 to a maximum of CNY5 million.

Jurisdiction	Requirements for trade secret protection
Singapore	To succeed in an action based on breach of confidence, the following need to be satisfied: 1. the trade secret must have the necessary "quality of confidence" about it; and 2. the trade secret must have been imparted in circumstances importing an obligation of confidence (an obligation of confidentiality can also be found where confidential information has been accessed or acquired without the company's knowledge or consent). If the above are established, breach of confidence will be presumed unless the individual alleged to be in breach can show that his or her conscience was unaffected e.g., if he or she came across the information by accident or was unaware of its confidential nature, or believed there to be a strong public interest in disclosing it. If breach of confidence is established, the owner of the trade secret can apply to the court for an injunction, seek either damages or an account of profits, and an order for delivery up and/or disposal of materials containing the trade secret.
Japan	The *Unfair Competition Prevention Act* (Act No. 47 of 19 May 1993) (UCPA) is the primary law applicable to protection of (a) trade secrets and (b) data for limited provision in Japan (a) In order to be protected as a trade secret under the UCPA, the information needs to satisfy the following requirements: 1. it must be kept and managed as a secret; 2. it must be technical or business information which is useful for business activities; and 3. it must not be publicly known (b) In order to be protected as data for limited provision under the UCPA, the information needs to satisfy the following requirements: 1. it must be technical or business data (excluding data which is treated as confidential); 2. it must be handled as data to be provided to specific persons on a regular basis; and 3. it must be accumulated in substantial quantities and managed by electronic, magnetic or other methods that cannot be recognised by human perception.
Australia	There is no legislation directly dealing with trade secrets in Australia. Parties affected by any disclosure of trade secrets may have a cause of action for breach of confidence or breach of contract. In order to protect trade secrets in Australia, parties should: 1. ensure they have a clear and well-drafted confidentiality agreement in place; 2. take steps to preserve confidentiality of material that is not in the public domain and has been identified as a trade secret, and share only when required for business purpose subject to a strict confidentiality regime or protocol as necessary; and 3. include confidentiality obligations in employment contracts to restrict disclosure to competitors.

RIGHTS UNDER CONTRACTS

2. RIGHTS UNDER CONTRACTS

Digital technologies and the rapid pace of development of these technologies are opening pathways to collaborative forms of innovation and realigning the focus on preventive measures around issues such as collaboration, licensing and the acquisition of technologies.

Contracts play an important role in the management of the legal problems of digitalisation, helping parties to find workable solutions in the private commercial environment especially when legislation in the field is developing apace. This is particularly relevant for trade secrets, data and IP protection and licensing, outsourcing, cloud computing, R&D co-operation and ventures, and insurance solutions. As technologies are increasingly being shared, we can expect companies to engage in cross-licensing activities particularly where each needs its own systems to be compatible with those of others.

2.1 Specific Technology Contract Considerations

Companies should give due consideration to properly structuring contract arrangements and terms to facilitate effective rights protection and enforcement. This should include taking into consideration local rules and practices relating to a range of issues where technology is involved and a contract will be agreed including any applicable legal and regulatory restrictions. Certain areas are of practical significance in litigating technology contracts, whether the contract concerns licensing, development, outsourcing or other forms of exploitation of technologies. The following are just some of these issues that may be encountered.

(a) **IP ownership:** Laws in most jurisdictions have provisions as to the default positions regarding ownership of new IP. Parties should consider whether such default rules are commercially appropriate, and try to agree and provide in the contract terms regarding the rights and obligations of assignment and use.

(b) **Technology standards:** (for example in the context of urban or smart mobility, where the interoperability of driverless cars, unmanned junction lights and traffic flow control must be assured for a safe and efficient transport system).

(c) **Licence or not:** A party may need a licence or right to sublicense IP that already exists or IP developed during the course of the commission or some other arrangement. The existence and scope of any right under a licence will have an impact on the availability of any interim relief pending any dispute on the suspension or termination of the agreement. In certain circumstances, and for commercial reasons, it may not be appropriate to grant a licence in respect of certain IP and, in such cases, the parties may consider agreeing on “non-assert” undertakings for the purpose of allowing the other party to use the IP. It should be borne in mind, however, that a non-assert undertaking is a contractual undertaking and likely to be non-binding on a successor-in-title.

(d) **Confidentiality:** There should be a clear agreement to treat any information relating to IP or improvements made to the IP as a trade secret. Information must be kept confidential and steps taken to ensure that employees understand and practise this.

(e) **Third-party licences:** Considerations should be given to any impact the transaction may have on existing licences. Where for instance the use of the IP is subject to third-party licensed IP, such a third-party licence may become terminable which may affect and give rise to disputes around either party's rights to use the IP.

(f) **Regulatory requirements:** Digitalisation is expected to become more heavily regulated in the coming years. Of late, some of the most significant regulatory developments involve cybersecurity and data usage and privacy. In the event of any regulatory breach, a properly drafted contract should enable the parties to identify the allocation of responsibilities as regards regulatory compliance and the handling of any incidents.

(g) **Exclusion of liability:** Many local laws have restrictions on the types of liabilities that may be excluded or limited by agreement.

(h) **Access right arrangements:** Data is a key component in technology contracts – consideration should be given to having in place adequate provisions on the use of any underlying data and newly created data, as well as having and gaining access to such data during the term of the contract or after termination.

(i) **The difficulty of guaranteeing supply:** Data as the currency of the digital economy can easily be hidden and its supply stopped at a push of a button.

(j) **Liability provisions:** Providing for parties' obligations and liabilities for cybersecurity, product liability claims, and IP infringement, and negotiation of scope of representations and warranties.

(k) **Warranties:** Given the inherent complexities of technology contracts, involving issues like interoperability, data and security, the role warranties and indemnities play in contractual arrangements is key. As a general rule, warranties should be specific, objective, meaningful, relevant, verifiable and not redundant.

(l) **Indemnities:** The applicability of indemnities requires careful thought in terms of the person or entity to whom the indemnity applies, the scope, the time, the subject matter, the triggering events and procedure as well as any cap on the indemnity. Not all breaches of contract will give rise to a right to claim an indemnity.

(m) **Termination for breach:** Whether or not a term is a representation, warranty, condition, fundamental term, promise or covenant will affect the remedies available to the innocent party. It is important when negotiating and drafting technology contracts to consider carefully whether or not the breach of a particular term, regardless of how it is labelled, is significant enough that it should entitle the

innocent party to a right to terminate. For some arrangements, termination of the agreement may be seen as a somewhat draconian penalty for any breach of contract, however minor, with the risk that this leads to a complete standstill of business operations. In appropriate circumstances, the parties may agree upon specific remedies for breach or disclaimer, or limitations on the remedies that may be available. For example, in the event of IP infringement, the licensor could be obliged to seek alternative licences for the licensee to enable the licensee to continue use of the IP; or alternatively, to repair defects at no additional charge.

(n) **Enforcement:** In order to counter difficulties in some jurisdictions, parties should consider arrangements to facilitate easier and more effective enforcement and deter non-compliance such as putting assets in escrow, call option rights, termination rights, taking security/pledge, and interim relief.

(o) **Insolvency/termination consequences:** Use of or rights to the IP may also be affected by there being any risk of a party's insolvency or bankruptcy, particularly for critical technology. Disputes may arise in respect of a party's entitlement to continuous use of the IP or rights to any IP sold by the liquidator to third parties. Proper drafting should take into account local insolvency rules and should be designed to protect the rights of parties in the event of the other party's insolvency. In appropriate circumstances, the parties should consider the appropriateness of escrow arrangements.

(p) **Governing law and jurisdiction:** **See Section 2.9.**

2.2 Types of Licences

When it comes to acquiring rights, standard licensing is carried out through written contracts, but there are various other licensing models that can also govern the shared use of technology. These include:

(a) Shrink wrap licences: commonly used in software that is purchased off the shelf according to standard conditions.

(b) Click wrap licences: in which the conditions of use are accepted by clicking on a message displayed on screen.

(c) Open-source software: encouraging right holders to share content under more open terms to encourage collaboration on and the dissemination of digital content and software – it is important to read any agreement thoroughly to ensure there are no other obligations or limitations on usage.

(d) Collective societies: collective licensing bodies represent the interests of their members in a particular industry.

(e) Smart Contracts: see our Talking Tech publication **Blockchain and its Application in the Field of IP: Smart Contracts and IPR Management**

2.3 What are the rights of the employee and employer when the employee creates technological content or innovations?

Jurisdiction	Ownership	Remuneration
Hong Kong	Copyright and aspects of know-how are generally involved in employee- created technological content and innovations. In general, where the content or innovation has been created in the course of an employee's employment, any resulting copyright or patent rights will belong to the employer. Employees can agree otherwise with their employers in respect of copyright but cannot do so for patents.	Where an employee creates an invention that results in a patent owned by the employer and certain conditions are met, an employee can apply to court for additional remuneration. The patent must, for instance, be shown to be of outstanding benefit to the employer. The court is required to consider various factors in determining this remuneration, including the benefit the employer has derived or may reasonably be expected to derive from the patent. For copyright, where an employee's work is exploited by the employer in a way that could not have been reasonably contemplated at the time of making the work, the employer must pay an award to the employee in respect of the exploitation. In the absence of agreement, the amount of the award can be determined by the Copyright Tribunal.

Jurisdiction	Ownership	Remuneration
China	An employer has rights and titles to inventions or technological achievements created by their employee either (1) by assignment to the employer or (2) as a result of the invention having been created and developed primarily using the employer's facilities and resources ("Employment Inventions"). The employer and the employee may enter into agreement concerning ownership, the terms of which will prevail. With respect to copyright, any work created by an employee in order to accomplish a task assigned to them by their employer will be regarded as an employment work. The copyright of the employment work vests in an employee except for the circumstances mentioned in the paragraph below, provided that the employer has the prior right to use the employment work within the scope of its business. Within the two years following the completion of such work, an employee may not authorise, without the consent of the employer, any third party to use the employment work in the same way in which it is used by the employer. In the following cases, in respect of works created during the course of employment, the right of authorship vests in the employee and all other rights of the copyright vest in the employer: 1. Drawings of engineering designs, drawings of product designs, maps, computer software and other works created during the period of employment, which are created mainly by using the material and technical resources of an employer and the responsibility for which is borne by the employer. 2. Work created during the course of employment in which the copyright vests in an employer pursuant to the provisions of a law, administrative regulation or contract. 3. Complications arise when it is not clear whether an inventor is an employee, such as in internship, secondment and university collaboration scenarios.	Employees who make important contributions to an Employment Invention are entitled to remuneration awarded by their employer. As required by the PRC Scientific and Technological Achievements Commercialisation Law (TCL), a statutory minimum remuneration is generally required to be paid to an employee unless (i) the employer has set out reasonable remuneration arrangements (including the amount, form and time of remuneration / rewards) in an agreement with the relevant employees or in its company policies or other public documents; and (ii) such remuneration arrangements have been made and implemented pursuant to and in accordance with the agreement and if involving company policies, in consultation with employees. In addition to the TCL, there are multiple laws and rules concerning employment inventions and remuneration matters in China (e.g., the current PRC Patent Law and its Implementation Rules), which take a similar approach to that of the TCL. Among the above laws and regulations, the TCL has the broadest scope as it is applicable to all R&D products, such as patented inventions, know-how, trade secrets, etc., while the PRC Patent Law will be only applicable to patentable inventions.

Jurisdiction	Ownership	Remuneration
Singapore	Employee-created technological content or innovation commonly involves works or subject matter in which copyright and patents can potentially subsist. With respect to patents, under Singapore law, assuming that there is no contract governing the issue of ownership of the invention, s 49 of the Patents Act provides that an employee's inventions will belong to the employer if: 1. the invention was made in the course of the employee's normal duties or in the course of duties falling outside their normal duties, but specifically assigned to them, and in circumstances where an invention might reasonably be expected to result from the carrying out of their duties; or 2. the invention was made in the course of the employee's duties and, at the time of the invention, because of the nature of their duties and particular responsibilities arising from the nature of their duties, the employee had a special obligation to further the interests of his employer's undertaking. Otherwise, any other invention is taken to belong to the employee. With respect to design, s4 of the Registered Designs Act (Cap. 266) provides that the owner of a design is usually the person who created the design, and they are entitled to apply for registration of the design. There are two notable exceptions to this general rule: 1. designs created in pursuance of a commission – unless there is an agreement to the contrary, where the commissioning party is treated as the owner; 2. designs created by an employee in the course of employment – unless there is an agreement to the contrary, the employer is regarded as the owner. With respect to copyright, s 134 of the Copyright Act provides that the employer or other person for whom the work was prepared is the initial owner of the copyright, unless there is a written agreement to the contrary.	Whether an employee has the right to be compensated by the employer for the invention depends on the terms of their employment contract.

Jurisdiction	Ownership	Remuneration
Japan	Under the *Patent Act* (Act No. 121 of 13 April 1959) (Patent Act), the right to obtain patent right(s), and the resulting patent right(s) themselves, to an invention of an employee vests in the employer from the moment they arise, if: • this is prescribed in advance in, for example, an agreement or employment regulation (Limb One); and • such invention (i) falls within the scope of the business of the employer, by nature of the said invention and (ii) was achieved by an act categorised as a present or past duty of the employee (Limb Two). If the above conditions are not satisfied, the employee will obtain ownership of the patent right. However, where Limb Two is met (but not Limb One), the employer will obtain a non-exclusive licence to the relevant patent and will not be required to pay the employee any compensation for such licence. The above rules also apply to a utility model right under the *Utility Model Act* (Act No. 123 of 13 April 1959) (Utility Model Act) and a design right under the *Design Act* (Act No. 125 of 13 April 1959) (Design Act). With respect to copyright, where a work is made: • by an employee; • in the course of his/her duty; • at the initiative of his/her employer, and • the work (except if such work is a computer program) is made public as a work of the employer's own authorship, so long as it is not provided for otherwise by way of contract, by virtue of the Copyright Act, the employer will be considered the author of the work and the owner of the copyright and the author's moral rights.	An employee is entitled to reasonable monetary compensation or other economic benefits from his/her employer for: 1. ownership of patent rights obtained by the employer as a result of Limb One and Limb Two being satisfied 2. ownership of patent rights obtained by the employer by way of transfer (whether by mutual agreement for an invention satisfying only Limb Two, or for an invention satisfying both Limb One and Limb Two but where the advance agreement provided for the employee to initially own the patent rights but is obliged to transfer within a specified time period) 3. an exclusive licence for the employer to patent rights for an invention satisfying Limb Two.

Jurisdiction	Ownership	Remuneration
Australia	The employer typically owns the IP created by the employee if it is related to the employer's business, unless the employment contract stipulates otherwise. In particular, s 35(6) of the Copyright Act 1968 (Cth) establishes a general rule that an employer will own the copyright in many types of works if they were created by an employee or apprentice. On the other hand, there is no such legislative equivalent in the Patents Act 1990 (Cth). Accordingly, it is the contractual relationship between an employer and employee that will determine matters concerning the ownership of inventions and the right to seek patents. In the absence of an express contractual provision dealing with the subject of ownership of inventions, a court may determine the matter by recourse to the principles of terms implied by law into the contract of employment. A research organisation may apply for a patent over an invention created by employees in the course of their employment. Although the Patents Act does not explicitly state this, s 15(1)(b) is generally relied upon by employers to claim proprietary rights in such inventions by virtue of their employment of the inventor, or by virtue of the terms of an employment contract. In particular, it has been noted that: "*It is an implied term of employment that any invention or discovery made in the course of the employment of the employee in doing that which he is engaged and instructed to do during the time of his employment, and during working hours, and using the materials of his employers, is the property of the employer and not of the employee*": *Victoria University of Technology v Wilson (2004) 60 IPR 392*. However, there have been suggestions that employers of university researchers or those in analogous organisations (as opposed to employees working for private sector commercial entities) may not necessarily have ownership of the patent if it was not necessary to imply the relevant term into the employment contract, and such a term will only be implied where there is a "duty to invent" as specified by the employment contract: *University of Western Australia v Gray* (2009) 179 FCR 346. In respect of the scope of the implied term that the invention is the property of the employer, it is necessary to show that the invention was created in the course of the employee's duties, and that it was created during the period when the employee was engaged by the employer.	In Australia, the entitlement of an employer to patentable information is governed by common law and equity. There is no applicable statute which governs the level of employee remuneration that must be received for an employer's use of an employee's invention. Accordingly, there are three main ways that an employee can receive remuneration for technological content and innovation: an express term of the employment contract between the parties; an implied term in the employment contract; or pursuant to a fiduciary obligation.

2.4 What issues relating to ownership of IP should be considered in commissioning and outsourcing arrangements?

Generally, the ownership of IP vests in the person making the invention or creating the IP (or persons claiming through them) unless otherwise provided by statute or agreed contractually. It follows that, generally, the owner of any IP to a commissioned work is the party who authored (in other words, created) the work. Therefore, in order for the commissioning party to use or own such work or IP, it must agree on the nature and scope of the proposed usage with the contractor in the commissioning contract.

A commissioning or outsourcing agreement should provide for and require the contractor to secure any necessary assignment or the relevant rights from inventors whether or not such inventors are employees of the contractor.

Other contractual rights (necessary for the non-owner) include the right to use the work (scope and duration of use) and the right to sublicense the use of the work to third parties. Parties are generally free to agree on the fee for a commissioned work.

In relation to copyright, there are moral rights (the right to make a work public, the right of attribution and the right to integrity) distinct from the copyright itself. Such rights are generally exclusive to the author and inalienable. Consequently, in order to take actions that relate to such rights, it is necessary to come to a contractual arrangement with the author.

Where there is no agreement, and subject to the requirements of local law, the commissioning party may be able to claim rights to the work depending upon the circumstances of the commission, including a licence or even an assignment. This may be, for example, in circumstances where the commissioning party has paid for the commission, and it is clear that the purpose of the commission is for the commissioning party to use the work to the exclusion of the contractor.

Specific local law issues – China

Generally, the PRC Civil Code allows parties to agree upon the ownership of technologies developed under a commissioning agreement. However, in the absence of any agreement, the ownership or rights to commissioned works are treated differently depending on the nature of the IP involved.

(a) **Copyright:** unless otherwise agreed, the copyright will vest in the party that has been commissioned to develop the technology (the commissioned party).

(b) **Patent:** unless otherwise agreed between the parties, the right to apply for a patent in respect of any patentable technology belongs to the commissioned party.

(c) **Know-how:** the default position is generally that both the commissioning and the commissioned party have the right to use and transfer the know-how created. However, the commissioned party may not transfer the know-how to a third party before delivering it to the commissioning party.

(d) It is noteworthy that under PRC laws the ownership of improvements to licensed technology and the IP therein rests with the licensee who created the improvements and the licensor cannot impose any obligation on the licensee to assign or license any improvements without charge.

2.5 Are there any implied warranties in technology contracts?

Jurisdiction	Ownership	Remuneration
Hong Kong	Terms can be implied into contracts in various ways: by law, custom or trade, and by the intention of the parties. The Sale of Goods Ordinance (Cap. 26) and the Supply of Services (Implied Terms) Ordinance (Cap. 457) are key statutes which imply terms and conditions into contracts for the provision of goods and services where the seller is selling in the course of business. For example, there is an implied term that goods are of merchantable quality (section 16, Sale of Goods Ordinance (Cap. 26)) which means the goods should be free from defects. In the case where a supplier is providing to a customer technological solutions which include software, however, this implied term is not always taken literally and some defects in code or 'bugs' may be viewed as acceptable. Other implied terms include (i) good title; (ii) quiet possession; (iii) quality; and (iv) fitness for purpose. Implied terms (i) and (ii) cannot be excluded by agreement but (iii) and (iv) can be excluded by agreement subject to the reasonableness test. It is settled by case law that the implied terms of good title and quiet possession include provision that the goods are free from IP infringement claims. Therefore, if there is an IP infringement claim against the products sold, then the implied terms would be breached. There is a similar statute for supply of services but, naturally, the implied terms are different as there is not necessarily any transfer of title of goods. The implied terms are: (1) care and skill; (2) time for performance; and (3) reasonable charge. These implied terms, however, can be excluded or restricted by agreement between the parties, subject to the reasonableness test and with notice except where it is a consumer contract (where one of the parties is not dealing in the course of business). The issue of IP infringement warranty / condition does not necessarily apply to a supply of services contract depending on the substance of the agreement (e.g., if the services are specifically for the creation of IP, then it would be arguable that it is an implied term under care and skill that the resulting IP should be free of any IP infringement claim). As it could be excluded by agreement, it would be advisable to exclude or restrict such condition / warranty and any liability relating thereto. The Sales of Goods Ordinance does not apply to the licensing and sale of IP per se.	To avoid uncertainty, parties are generally free to exclude implied terms and warranties from contracts. However, there are statutes which restrict such exclusions. For example, the Control of Exemption Clauses Ordinance (Cap. 71) provides that a seller's implied undertakings as to title etc. may not be excluded or restricted (section 11). Also, a party may not exclude or restrict liability for death or personal injury resulting from negligence, and exclusion or restriction of liability for other loss or damage resulting from negligence must satisfy the requirement of reasonableness

Jurisdiction	Ownership	Remuneration
	Terms and conditions can also be implied by the courts provided the following conditions must be satisfied: the term or condition (1) must be reasonable and equitable; (2) must be necessary to give business efficacy to the contract; (3) must be obvious such that 'it goes without saying'; (4) must be capable of expression; and (5) must not contradict any express term of the contract. There have been English cases which suggest that where a supplier is providing 'standard' (rather than custom-made) technological software and solutions, it is implied that customers have an obligation to specify any special needs to the supplier and devote time to familiarise themselves with the software. The terms to be implied in each situation will depend on the circumstances.	
China	There is a mandatory rule under the PRC Civil Code that an assignor or a licensor must warrant that it is the legal owner of the technology to be assigned or licensed, the assigned or licensed technology is accurate and complete, and that it can satisfy the agreed purpose. More generally, the PRC law imposes certain quality warranties for consumer goods.	As for a seller's warranty regarding the quality of goods sold to consumers, the seller may exclude its liability in relation to a defect in such goods (save for food or drugs) if the defect had been known to the consumer before the sale took place and the defect does not violate any PRC mandatory rules.
Singapore	Under Singapore law, contractual terms such as warranties can either be implied in fact or by operation of law. Terms will only be implied in fact if they are necessary to give business efficacy to the contract and if they are so obvious that a third party if asked by the parties, at the time the contract was concluded, whether they intended for the term to be included in the contract would have said "oh, but of course" (the Officious Bystander Test). Unlike the implication of terms in fact, the implication of terms in law is concerned with considerations of fairness and policy rather than the intentions of the parties. To that end, when the court implies a term in law, it lays down a general rule that certain terms will be implied in all contracts of a defined type unless it would be contrary to the express words of the agreement to do so. Some warranties are implied by law by virtue of the statutory provisions in the Sale of Goods Act (Cap. 393). For instance, section 14 of the Sale of Goods Act sets out the implied terms about quality or fitness of particular goods supplied. However, these implied terms do not apply to any licensing or assignment of IP. It is also possible for terms to be implied by custom based on the common practice of the specific trade. However, implication by custom is less frequently used in Singapore and relevant evidence of such custom has to be provided.	Parties can, to the extent statutorily allowed, contractually exclude implied terms and warranties. Examples of statutes which prohibit the contractual exclusion of implied terms and warranties include the Sale of Goods Act, which provides that conditions implied under sections 13, 14 and 15 (correspondence with description, satisfactory quality, fitness for purpose and sale by sample) cannot be excluded or restricted as against a person dealing as a consumer.

Jurisdiction	Ownership	Remuneration
Japan	Under Japanese law, the *Civil Code* (Act No. 89 of 1896, as amended) (*Civil Code*) provides for certain warranties (for example, defect warranties) to apply to contracts generally (Article 562, 563 and 565 of the *Civil Code*) and these provisions may also apply to licence agreements. There are no specific conditions which a party must satisfy to rely on the statutory warranties. However, there is some uncertainty about the application of these provisions to intellectual property rights and, if they do apply, the result of such application. For example, given the Civil Code provides statutory warranties with respect to liability for "incompatibility with the agreement", within the realm of intellectual property there is uncertainty as to what constitutes "incompatibility".	The provisions of the Civil Code are not mandatory, and their application can be expressly excluded by agreement. In addition, it is possible that a Court may view that, on the facts of any particular case, the statutory warranties are not applicable, with the consequence that the seller will not bear any liability pursuant to the warranties. Accordingly, it is common for parties to include, as a minimum, warranties in their agreements which concern the following matters: 1. authority to license 2. non-existence of licensing restrictions 3. technological benefit of the licensed object 4. validity of the technology right 5. existence of the technology right (including the maintenance and management of the right) 6. non-infringement of the rights of third parties
Australia	Terms can be implied into contracts in various ways: by law, custom or trade, and intention of the parties. Terms and conditions can be implied provided the following conditions must be satisfied. The term or condition must: 1. be reasonable and equitable; 2. be necessary to give business efficacy to the contract; 3. be so obvious that 'it goes without saying'; 4. be capable of expression; and 5. not contradict any express term of the contract.[3] Under the Australian Consumer Law (ACL), automatic consumer warranties apply to the supply of many products and services. In particular, businesses that sell, hire or lease products and services for under AU$40,000 (or over AU$40,000 if the products or services are normally purchased for personal or household use) must guarantee that those goods:	Parties can agree to the exclusion of certain liability however parties should consider that Australian courts will take into consideration the bargaining power of each of the parties in determining whether an exclusion clause is fair and equitable (or conversely, unconscionable). The ACL limits a party's ability to exclude consumer warranties and rights. Consumer guarantees and liability for manufacturers for goods with safety defects cannot be excluded. Actionable remedies available under the *Competition and Consumer Act 2010* (Cth) can also not be excluded or limited. Further, the right for a consumer to terminate unsolicited consumer agreements cannot be excluded.

3 *Codelfa Construction Pty Ltd v State Rail Authority of NSW* (1982) 149 CLR 337.

Jurisdiction	Ownership	Remuneration
	1. are of acceptable quality (i.e., the goods must be safe, lasting, have no faults, look acceptable and do all the things someone would normally expect them to do); 2. are fit for purpose; 3. have been accurately described; 4. match any sample or demonstration model; 5. satisfy any express warranty; 6. have a clear title, unless otherwise advised to the consumer before the sale; and 7. have spare parts and repair facilities reasonably available for a reasonable period of time, unless the consumer is advised otherwise. Manufacturers and importers have to guarantee that their goods: 1. are of acceptable quality; 2. have been accurately described; 3. satisfy any manufacturer's express warranty; and 4. have spare parts and repair facilities reasonably available for a reasonable period of time, unless the consumer is advised otherwise. Businesses that supply services have to guarantee that those services will be: 1. provided with due care and skill; 2. fit for any specified purpose (express or implied); and 3. provided within a reasonable time. When the above warranties / guarantees are breached, customers can seek compensation for damage and losses they have suffered provided that the damage was reasonably foreseeable. The definition of "goods" under the ACL includes "computer software". The Federal Court has recently found that the supply of digitally downloaded computer software is a supply of a good and thus carries the warranties for goods under the ACL.[4]	

4 *Australian Competition and Consumer Commission v Valve Corporation (No 3)* [2016] FCA 196.

2.6 Are there any restrictions or formalities on the licensing of technology rights?

Jurisdiction	Restrictions or formalities
Hong Kong	A licensor may only license use of technology rights it owns. Although terms in a licence can be commercially agreed between the parties, licensors are generally advised to include provisions relating to the quality of products and services produced by their licensees. It is recommended that licences involving patents or patent applications be in writing and registered with the Patents Registry. An unregistered licence is not effective against third parties acquiring a subsequent, conflicting interest in the patent or patent application without knowledge of the earlier licence. A licence is binding on the licensor's successors in title in the copyright, except a purchaser in good faith for valuable consideration and without notice of the licence or a person deriving title from such a purchaser. Recordals are not required for copyright licences. However, for exclusive licensees of copyright to take advantage of protection under the Copyright Ordinance (including against any successors in title), the exclusive licence will need to be in writing and signed by or on behalf of the copyright owner. Where trademarks are also involved, a licence is not effective unless it is in writing and is signed by or on behalf of the licensor. The licence will bind successors in title to the licensor's interest unless the licence provides otherwise. The licence should be recorded with the Trademarks Registry as soon as possible otherwise the licence will not be effective against a person acquiring a conflicting interest in ignorance of the transaction. If the licence is not recorded within six months, the licensee will not be entitled to damages or an account of profits for infringements in the period before the licence is recorded.

Jurisdiction	Restrictions or formalities
China	Technology contracts whereby parties prescribe their rights and obligations in respect of the development or transfer of technology are subject to various statutory provisions. One provision worth noting is the prohibition on imposing unfair conditions on grant-backs of improvements to technology. Technology contracts that illegally raise monopoly concerns or infringe on the technology of a third party are also otherwise invalid. Parties are free to contract as to the ownership of improvements; however, grant-backs that impose unfair conditions are not permissible where no proper compensation is provided or the non-reciprocal transfer of technology is involved. There are additional requirements and restrictions that cannot be imposed in respect of technology contracts. For example: 1. requiring the party accepting the technology to accept conditions for exploitation of the technology including purchasing any technologies, raw materials, equipment, products or services which are not essential for so exploiting; 2. unreasonably restricting the channels or sources where the party accepting the technology may purchase raw materials, components, products or equipment (e.g., a provision requiring purchases of raw materials only from a designed source without justification); 3. impeding the exploitation of technology according to market demand including unreasonably restricting quantity, product types, price, sales channels and export markets of the subject technology (e.g., a provision requiring export to a designated party); 4. restricting one party from obtaining similar or competitive technologies from other sources; and restricting one party from research and development on the subject technology or using such improved technology. Requirements and restrictions equivalent to those above have been removed from the Administrative Regulation on Technology Import and Expert (TIER), but are still provided for in other law, administrative regulation and judicial interpretation. There are recordal or approval requirements in respect of technology imports or exports depending on the classification of the technologies in the Catalogues of Technologies Prohibited or Restricted to be Imported/Exported into/out of China. The catalogue divides technologies into three categories: 1. Prohibited – imports or exports of such technology are prohibited and the agreement is not effective in China 2. Restricted – imports or exports of such technology are only allowed after approval has been obtained from the Ministry of Commerce (MOFCOM). The agreement is not effective until it is approved 3. Unrestricted / free – if the technology is not listed as prohibited or restricted, then it is considered "free" to be imported / exported and only registration of the agreement with MOFCOM is required. The agreement is effective upon execution of the parties The Chinese party is responsible for the registration or approval process and, in order to be able to do so, the Chinese party must have the relevant contractual import / export rights. In addition, in respect of any registered technology rights, such as a patent right, the parties must record the licence agreement in relation to the patent right with the PRC Patent Office within three months after the licence agreement takes effect. As required by the PRC Civil Code, a technology licence agreement has to be made in writing between the parties.

Jurisdiction	Restrictions or formalities
Singapore	Generally, intellectual property right licences have to be in writing in order to be effective. 1. For trademarks, this is explicitly provided for in s42(3) of the Trade Marks Act (Cap. 332) 2. For registered designs, the requirement is implicit as the signature of the grantor of the licence is required 3. For copyright licences, it need not be in writing but for an assignment of such copyright to be valid, it would require that the assignment be made in writing and signed by or on behalf of the assignor. An exclusive copyright licence would also need to be in writing, and signed by or on behalf of the owner. 4. For patent licences, it need not be entered in a particular form. However, for licences not to be performed within one year of the agreement, the Civil Law Act stipulates a writing and signature requirement for such agreement to be effective, hence it is generally recommended that patent licences be in writing. 5. Unregistered rights such as unregistered trademarks and know-how or confidential information may be licensed in accordance with general contract law principles. In the case of registrable intellectual property rights, licences are registrable transactions. It is important to make the application for the registration of the prescribed particulars of a registrable licence, otherwise the licence will be ineffective against a person acquiring a conflicting interest in the right in ignorance of the licence. • There are statutory limitations as to a right in damages or an account of profits in respect of any infringement of the registered design or patent occurring after the date of the licence and before the date of application for the registration of the particulars of the licence. • For infringements occurring after the licence is executed, the transaction must be registered within six months of the date of the transaction, unless the court is satisfied that it was not practicable to register it in that period. • For trademarks, the transaction will not be considered ineffective against a person who acquires a conflicting interest in or under the registered trademark in ignorance of a licence that has not been recorded. The trademark proprietor can still pursue a claim for damages, an account of profits or statutory damages in respect of any infringement of the registered trademark that occurs after the date of the transaction and before the date of the recordal of the licence. There are also compulsory licensing provisions in the Patents Act and statutory licensing provisions in the Copyright Act which require the licensing of patents and copyright works to be granted under certain conditions.

Jurisdiction	Restrictions or formalities
Japan	Under Japanese law, in principle, licence agreements are not required to be in writing. However, certain licences of intellectual property rights are required to be registered in order to be effective and thus, for the registration process, the licence agreement needs to be in writing. 1. With respect to patent rights, utility model rights and design rights, an exclusive licence is required to be registered to be effective and must therefore be in writing for the registration process. On the other hand, a non-exclusive licence is not required to be registered to be effective (and thus does not need to be in writing). A non-exclusive licence is binding on a successor in title to the right if succession occurred after such licence was granted 2. With respect to trademarks, an exclusive licence is required to be registered to be effective and a non-exclusive licence is required to be registered for perfection of the licence. In both cases, the licence agreement needs to be in writing for the registration process 3. With respect to copyright, since it arises automatically at the time the relevant work is produced, there are no writing requirements or registration requirements for obtaining copyright licences, although certain items can be voluntarily registered for the purpose of visibility. On the other hand, a publishing rights licence is binding on a successor in title only if it is registered. For the purpose of the registration process, the licence agreement needs to be in writing. However, a copyright licence, as well as an unregistered publishing rights licence, is not binding on a successor in title to the copyright.
Australia	Licences may be granted by the owner of relevant IP rights or by a party that has been authorised by the owner to grant such rights. Whilst most restrictions will be reflected in the drafting of the licence itself, the type of licence granted will also affect what restrictions are associated with the licence: 1. For a non-exclusive licence, the licensor has the right to grant other licences; 2. For a sole licence, the licensor can only grant one party the relevant rights, but also reserves the right to itself to exercise the relevant rights; and 3. For an exclusive licence, the licensor grants only one party the relevant rights and agrees not to exercise those rights itself. Exclusive licences do not always provide blanket protection for the licensee. The IP owner can place restrictions that limit the licence, such as: product restrictions (that restrict the licensee's use of the IP to a particular class of product); field restrictions (that restrict the licensee to a specific field of application); and/or territory restrictions (that restrict the licensee to a specific geographical area) In addition, where there is joint ownership, the consent of both owners is required to grant a licence to a third party.

2.7 Are there any restrictions or formalities on the assignment of technology rights?

Jurisdiction	Restrictions or formalities
Hong Kong	The owner may only assign technology rights it owns. Rights in a patent application or registration may be assigned. The assignment must be in writing and signed by or on behalf of the assignor for the assignment to be effective. Assignments should also be recorded as soon as possible otherwise third parties acquiring a subsequent, conflicting interest in the patent or patent application without knowledge of the assignment will have rights against the new owner. Copyright, including future copyright, may be assigned in full or in part (including for part of the period during which copyright subsists). An assignment of copyright must be in writing and signed by or on behalf of the assignor to be effective. Trademark applications and registrations may also be assigned in full or in part. An assignment is only effective if it is in writing and signed by or on behalf of the assignor. The assignment should be recorded with the Trademarks Registry as soon as possible otherwise the assignment will not be effective against a person acquiring a conflicting interest in ignorance of the transaction. If the assignment is not registered within six months, the new owner will not be entitled to damages or an account of profits for infringement during the whole of the period before the assignment is recorded.
China	An IP assignment agreement must be made in writing between the relevant assignor and assignee. Change of a patent right owner or a patent applicant must be recorded with and approved by the PRC Patent Office. Assignment of copyright also needs to be made in writing and signed by the relevant assignee and assignor. Copyright registration is not mandatory under PRC law but a copyright registration certificate will serve as prima facie evidence of copyright in PRC legal proceedings.
Singapore	For an assignment of copyright (whether total or partial) to be valid it must be in writing and signed by or on behalf of the assignor (the copyright owner). An assignment can also be entered into in respect of copyright that has yet to come into existence, in which case the assignment will only be effective to transfer ownership of the copyright as soon as the work is created. The assignment of a patent or any right in a patent or application as well as any assent relating to any patent, application or right will be void unless it is in writing and signed by or on behalf of the parties to the transaction. Any person who claims to have acquired the property in a patent or an application for a patent by virtue of any transaction, instrument or event (collectively, transaction) should register the transaction with the Registrar of Patents, failing which their rights are restricted as against an infringer and any person acquiring a conflicting interest in the invention in ignorance of the transaction. A registered trademark may be assigned by the registered proprietor as such, absolutely or by way of security. Such dealings should be registered with the Registry of Trademarks; an unregistered assignment is ineffective as against a person acquiring a conflicting interest in the trademark in ignorance of it. Other unregistered rights, such as unregistered trademarks and confidential information or know-how may be assigned in accordance with general contract law and common law principles.

Jurisdiction	Restrictions or formalities
Japan	IP rights are generally transferable. Under Japanese law, in principle, the assignment of IP rights is not required to be in writing. However, in order for a transfer to be effective (between the parties and as against third parties), a transfer of patent rights, utility model rights, trademark rights and design rights must be registered with the Japan Patent Office, and such process requires the transfer to be evidenced in writing. With respect to copyright, registration at the Agency for Cultural Affairs (or for computer programs, at the Software Information Centre) is required for the perfection of a copyright transfer.
Australia	Generally, technology rights can be assigned to third parties through express or implied assignments like any other property. Section 196(3) of the Copyright Act 1968 (Cth) stipulates that assignments of copyright must be in writing, signed by or on behalf of the assignor, although an informal assignment may be given effect in equity. No particular form of words is required, but an intention to effect an assignment of copyright must be evident. A person who acquires a limited copyright as a result of a partial assignment is treated as the owner of a separate copyright for that particular purpose under s 30 of the Copyright Act 1968 (Cth). Where future copyright is assigned, the relevant copyright vests in the assignee or the assignee's successor upon coming into existence, provided at that time no other has a better claim (under s 197(1) of the Copyright Act 1968 (Cth)). In relation to patents, s 13(2) of the Patents Act 1990 (Cth) provides that the exclusive rights created by a patent are personal property and capable of assignment and devolution by law. Section 14 provides that an assignment of a patent must be in writing signed by or on behalf of the assignor and assignee, and that a patent may be assigned for a part of the patent area. Patents can also be assigned for a limited period of time. In addition, under s 16(1), a co-owner of a patent cannot assign an interest in the patent without the consent of the other co-owners.

2.8 Can a technology right be mortgaged or pledged?

Jurisdiction	Restrictions or formalities
Hong Kong	Security is available over IP rights. Generally, security over IP can be taken by a charge (fixed or floating) or a mortgage (assignment). A fixed charge is usually preferable to mortgage (assignment). The secured creditor will usually require the security provider to continue to renew and exploit the IP to maintain its value. Copyright can be secured but, as copyright is not registrable, it is unclear how effective the security is. In the case of a company, the company must deliver a statement of particulars of the security together with a certified copy of the instrument creating or evidencing the security to the Companies Registry for registration within one month of the date the security is created, or, where the security is created outside Hong Kong and comprises property situated outside Hong Kong, within one month after the date on which a certified copy of the instrument creating or evidencing the security could, if despatched with due diligence, have been received in Hong Kong in due course of posting, failing which the security is void against a liquidator and any creditor of the company. The security should also be registered at the relevant registry: 1. for trademarks, at the Trademarks Registry: registration should be made as soon as possible and in any event within six months from the date the security is created 2. for patents, at the Patents Registry: registration should be made as soon as possible and in any event within six months from the date the security is created 3. for registered designs, at the Designs Registry: registration should be made as soon as possible and in any event within six months from the date the security is created Failure to register within the six-month period can limit the remedies available to the secured creditor if the IP right is infringed. Also, until an application has been made for registration of the security, the grant of the security is ineffective as against a person acquiring a conflicting interest in the IP in ignorance of the grant.
China	Pursuant to the PRC Security Law, exclusive rights of trademarks, property rights among patents and copyrights that are transferable by law are allowed to be pledged. The pledgor and the pledgee must conclude a written contract in respect of such intellectual property rights and register the pledge with the competent authorities for the administration of the trademark, patent or copyright. The pledge contract shall become effective on the date of registration. Taking a patent right, for example, where a patent is pledged, the pledgor and the pledgee must jointly register / record the pledge at the PRC Patent Office, and must cancel the pledge registration / recordal with the PRC Patent Office when an obligor has fulfilled its debt obligations, when a pledge right has been realised, or when a pledge right is terminated for other reasons.

Jurisdiction	Restrictions or formalities
Singapore	Security over IP rights can be granted by a mortgage or by a fixed or floating charge. In respect of copyright, the assignment must be in writing and signed by or on behalf of the assignor. In respect of a patent, an assignment must be in writing and signed by or on behalf of the parties to the transaction. Where a body corporate is involved, the assignment or mortgage must be signed by, or be under the seal of, the body corporate. In the case of a mortgage, there must be a proviso for reassignment on redemption. The assignment or mortgage must be registered in order to be enforceable against any other person who subsequently claims to have acquired an interest in the registered patent. In respect of a trademark, an assignment must be in writing and signed by or on behalf of the assignor or their personal representative. If the assignor or personal representative is a body corporate, this requirement can be satisfied by the affixing of its seal. The assignment or grant of security over a trademark must be registered in order to be enforceable against any other person who subsequently claims to have acquired an interest in or under the trademark. In relation to a charge that is created by a company incorporated in Singapore (or the Singapore-registered branch of a foreign corporation), a charge on a patent or licence under a patent or on a trademark, or on a copyright or a licence under a copyright, the charge must be lodged with the Registrar of Companies for registration: 1. within 30 days after the creation of the charge in the case where the document creating the charge is executed in Singapore; and 2. within 37 days after the creation of the charge in the case where the document creating the charge is executed outside Singapore
Japan	**Patent right, utility model right and design right** In order for a pledge over a patent right, utility model right, design right or an exclusive licence to any of those types of rights to be effective (between the parties and as against third parties), the pledge must be registered. Once registered, the pledge is binding on a successor in title to the right. On the other hand, a pledge over a non-exclusive licence for the aforementioned types of rights is not required to be registered to be effective and, further, without registration, it is binding on a successor in title to the right if succession occurred after the relevant licence was granted. **Trademark right** In order for a pledge over a trademark right or an exclusive licence for a trademark right to be effective (between the parties and as against third parties) as well as for a pledge over non-exclusive licences for a trademark right to be perfected against third parties (i.e., perfection of a pledge), the pledge must be registered. Once registered, a pledge is binding on a successor in title to the right. **Copyright** In order for a copyright pledge to be perfected against third parties, the pledge must be registered. Once registered, a pledge is binding on a successor in title to the copyright. **Attachment** A creditor of an owner of IP rights may apply to the court to attach the IP rights for enforcement of their monetary claims against the owner. Upon attachment, the owner is prohibited from transferring or pledging the IP rights, the court will sell the attached IP rights and the owner will lose ownership of them.

Jurisdiction	Restrictions or formalities
Australia	Goodwill, trademarks, patents, registered designs and copyright may be mortgaged or charged. A security interest such as a mortgage or exclusive licence can be taken out on intellectual property such as a patent, registered design or trademark (see s 10 of the *Personal Properties Securities Act 2009* (Cth)). All interests in relation to property require registration via the national online database, Personal Property Securities Register (PPSR).

2.9 How do I choose the governing law for my technology contracts?

When choosing a governing law for your technology contracts, you should consider the following:

(a) Whether the technology is a type of IP which may be protected by registration. If so, you may wish to consider whether it would be appropriate to have the contract governed by the law of the same jurisdiction in which the technology has been registered for protection. It would naturally be more difficult to do so if IP registered in more than one jurisdiction is involved (Registration Jurisdictions). In any event, you should bear in mind that irrespective of the governing law of the contract, the validity and enforceability of the IP itself will remain subject to the law of the Registration Jurisdiction. The same will probably apply to unregistered IP.

(b) Whether the jurisdiction has any legislation or regulations governing the ownership, use or exploitation of the technology in question and, if so, whether such legislation or regulations are in your favour. In addition, consideration should also be given to any obligations which may be imposed on owners or users of the technology and whether such obligations are operationally onerous.

(c) Whether the laws of that jurisdiction provide for contractual certainty. If it is a common law jurisdiction, the latest body of case law dealing with the subject technology should be reviewed to ensure that there are no adverse developments.

(d) Where you intend to enforce the contract. Consideration should be given to any issues that may arise should you wish to enforce in a different jurisdiction than that making judicial orders regarding the contract.

2.10 Can technology and digital rights disputes be arbitrated?

Jurisdiction	Restrictions or formalities
Hong Kong	Hong Kong introduced amendments to the Arbitration Ordinance in 2017, clarifying that disputes over the subsistence, scope, validity, ownership and/or infringement of intellectual property rights may be resolved by arbitration and that it is not contrary to Hong Kong public policy to enforce arbitral awards involving intellectual property rights.
China	Contractual IP disputes in relation to technology and digital rights – for example, disputes arising from IP licence or assignment agreements, technology development or service agreements, publication agreements, etc. – are generally arbitrable in China. It is arguable that IP infringement and validity disputes can be submitted for arbitration in China, but any decision would be binding on the contracting parties only.

Jurisdiction	Restrictions or formalities
Singapore	Any dispute is generally arbitrable in Singapore, unless it is contrary to the public policy of Singapore to do so. Previously, it was unclear whether patent disputes could be arbitrated in Singapore given concerns about public interest, but the Intellectual Property (Dispute Resolution) Act 2019 now provides that IP rights and disputes are arbitrable by amendments to the Arbitration Act 2001 and International Arbitration Act 1994.
Japan	Under the Arbitration Act (Act No. 138 of 2003, as amended) (Arbitration Act), arbitration agreements in respect of civil disputes (except for certain family law matters) are enforceable (Article 13(1) of the Arbitration Act). This means that a dispute concerning alleged infringement of a contractual right in relation to technology or intellectual property is, as a general rule, arbitrable. In Japan, in addition to general arbitral institutions (notably the Japan Commercial Arbitration Association (JCAA)), there is an arbitration institution specialising in intellectual property rights – the "Japan Intellectual Property Arbitration Center". More recently, the Japanese government has sought to further develop Japan as a hub for patent and trademark dispute resolution through the establishment of the International Arbitration Centre in Tokyo (IACT) which markets itself as having an IP focus.
Australia	Technology and digital rights disputes can be arbitrated in Australia, save that granting a patent, or the making of declarations as to eligibility with respect to patent applications, are matters which are non-arbitrable. Arbitration, as a private and confidential procedure, is increasingly being used to resolve disputes involving IP rights, especially when involving parties from different jurisdictions. The Arbitration and Mediation Center of the World Intellectual Property Organization (the WIPO Center) provides a range of services designed to resolve international disputes for IP and technology including arbitration and expedited arbitration.

2.11 How do I choose between litigation, arbitration and other forms of alternative dispute resolution when concluding my contract?

The most appropriate form of dispute resolution in respect of technology contracts will depend, among other things, on the following considerations:

(a) Reputation of the seat of arbitration – in choosing the seat of arbitration, parties should consider the effect that this might have upon the conduct of the arbitration and the potential enforceability of the award.

Jurisdiction	Consideration
Hong Kong	Hong Kong has a strong reputation as a seat of international arbitration due to good hearing facilities, availability of quality arbitrators familiar with the seat, internationally renowned arbitral institutions (HKIAC and ICC), arbitration-friendly rules and laws, and an independent judiciary which supports arbitration.
China	The best-known arbitral institution in China is the China International Economic and Trade Arbitration Commission (CIETAC) in Beijing. Courts in China have greater powers to assume control over disputes and the conduct of the arbitration.
Singapore	Singapore is well-known as a pro-arbitration jurisdiction. There is strong support in terms of judicial endorsement, infrastructure and facilities. A popular arbitral institution based in Singapore is the Singapore International Arbitration Centre.

Jurisdiction	Consideration
Japan	Japan is an arbitration-friendly jurisdiction, with arbitration legislation based on the *UNCITRAL Model law on Commercial Arbitration* (UNCITRAL Model Law). Japan is also a signatory to the *New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards* (New York Convention). Local courts are empowered to support arbitration in, for example, the taking of evidence. The local Japanese arbitral institution that administers international arbitrations is the Japan Commercial Arbitration Association, which has a modern set of rules for arbitration, including expedited procedure rules. Recently, the Japanese government has taken various steps to increase the attractiveness of Japan as a seat for arbitration, including the relaxation of the regulatory regime for foreign lawyers participating in arbitration proceedings, as well as investing in dedicated arbitration facilities in the form of the Japan International Dispute Resolution Centre.
Australia	Australia is a pro-arbitration jurisdiction where the courts have a track record of supporting arbitration and enforcing arbitral awards. The *International Arbitration Act 1974* (Cth) is based on the UNCITRAL Model Law and Australia is a signatory to both the New York Convention and the International Centre for Settlement of Investment Disputes (ICSID) Convention. The Australian Centre for International Commercial Arbitration (ACICA), the national arbitration institution which was established in 1985, is the sole default appointing authority competent to perform the arbitrator appointment functions under the International Arbitration Act 1974 (Cth).

(b) Need for and availability of adjudicators with specialist expertise

Jurisdiction	Consideration
Hong Kong	The HKIAC has established a special panel of arbitrators for IP disputes. The panel is made up of members from a variety of backgrounds (with experience from more than 10 jurisdictions and from different professions, including in-house counsel, senior counsel, former judges and university professors). These arbitrators have expertise in IP matters including licensing issues, copyright infringement, and patent, trademark and design prosecution matters.
China	CIETAC has published a set of procedural rules for resolving disputes in relation to the registration or use of domain names administered by the China Internet Network Information Center. According to these rules, domain name disputes submitted to CIETAC will be decided by a panel consisting of one or three independent experts who have relevant legal knowledge about the internet. CIETAC has established a special panel of IP experts with relevant expertise.
Singapore	If litigation is chosen, there is a list of specialist IP judges at the Singapore High Court. If arbitration is chosen, parties may wish to nominate arbitrators with specialist knowledge to adjudicate the dispute. The Singapore International Arbitration Centre (SIAC) has established a panel of 19 IP specialist arbitrators, which includes internationally renowned IP experts. In addition, WIPO has established an Arbitration and Mediation Centre (AMC) in Singapore, its only centre outside Geneva. A collaboration framework between the Intellectual Property Office of Singapore (IPOS) and the WIPO AMC allows parties to resolve IP disputes via alternative dispute resolution (ADR) at the WIPO AMC.
Japan	If arbitration is chosen, parties can nominate arbitrators who specialise in the relevant technology or area of intellectual property. There is an increasing number of suitably qualified local and international practitioners based in Japan who accept appointments as adjudicators or arbitrators in this area.

Jurisdiction	Consideration
Australia	Australia is known worldwide for having a large number of high-profile international arbitrators. Parties can nominate arbitrators who specialise in the relevant technology or area of intellectual property. There is no dedicated IP arbitrator panel; however, arbitrators specialising in IP, brands and trademarks can be located through various arbitral bodies (such as ACICA, Chartered Institute of Arbitrators (CIArb) (Australia branch) and Resolution Institute, formerly known as The Institute of Arbitrators & Mediators Australia). The International Chamber of Commerce (ICC) Arbitrator Appointments Committee selects arbitrators for ICC arbitrations (where required by the parties) and will usually endeavour to choose an arbitrator with relevant sector experience. In addition, if mediation is a path the parties choose to take, IP Australia provides an IP Mediation Referral Service which provides a route for parties to contact specialist IP mediators.

(c) Availability of specialist IP Courts or Judges

Jurisdiction	Consideration
Hong Kong	The Hong Kong courts established in 2019 a formal IP list which is overseen by a specialist judge and other designated judges. There are particular court rules and directions which focus on making IP cases more efficient.
China	There are specialist IP courts in major cities presided by specialist IP judges.
Singapore	The Singapore courts have specialist IP judges. There is also an IP Court Guide which sets out special case management procedures for IP cases.
Japan	Japan has specialist courts which have expertise in intellectual property rights (and some kinds of disputes regarding certain intellectual property rights are subject to the exclusive competency of those courts)
Australia	Australia's Federal Court has identified Intellectual Property National Practice Area judges in each state and territory. They specialise in Patents & Associated Statutes, Trademarks, or Copyright & Industrial Design.

(d) Need for confidentiality

Jurisdiction	Consideration
Hong Kong	The Arbitration Ordinance (Cap. 609) includes provisions which protect the confidentiality of arbitral proceedings and any awards. The HKIAC Rules also contain provisions for confidentiality. Litigation proceedings are generally accessible to the public.
China	According to CIETAC rules, the tribunal will review a case in private session unless otherwise required by the parties. For cases reviewed in camera, arbitrators, witnesses, translators, experts and other related parties must not disclose case-related information to any third parties. Evidence involving state secrets, trade secrets or private personal information will be kept confidential. If such evidence needs to be presented in a court proceeding, such evidence will be presented in private session.
Singapore	The SIAC rules contain provisions for confidentiality. Litigation proceedings are generally accessible to the public.

Jurisdiction	Consideration
Japan	Arbitration proceedings in Japan are generally regarded as confidential; however, best practice is to expressly agree that the process will be private and confidential (assuming this is the intention of the parties). Where the arbitration is governed by the JCAA rules, Article 42 imposes confidentiality obligations on the parties, counsel and the tribunal.
Australia	Confidentiality will be governed by the arbitration agreement or clause of a disputed contract between the parties. Arbitration may be preferred to litigation as it allows parties to keep the proceedings private and confidential. This may be of importance where the dispute concerns trade secrets or commercial information of value to a competitor. The confidentiality regime under the *International Arbitration Act 1974* (Cth) (at ss. 23C-23G) applies by default to international arbitrations seated in Australia and arising from arbitration agreements made on or after 14 October 2015. For arbitral proceedings arising from agreements prior to 14 October 2015, the confidentiality regime applies on an "*opt in*" basis. The ACICA Rules (2021) also contain provisions for confidentiality under Article 26. In the case of litigation, the existence of proceedings is generally of public record and hearings are often open to the public, although in certain circumstances an application for confidentiality in respect of part or all of the hearings can be made. Parties can ensure that any highly sensitive commercial information is only disclosed subject to a strict confidentiality regime which will keep the information, and any documents referencing it, from the public record.

(e) Ease of enforceability

Jurisdiction	Consideration
Hong Kong	Hong Kong court judgments may be enforced through charging orders, writs of execution or garnishee, insolvency or contempt proceedings. Foreign court judgments are enforced in Hong Kong either through a simplified statutory registration regime or under common law. As far as enforcement of Mainland Chinese court judgments is concerned, there is a reciprocal arrangement for enforcement of certain types of court judgments (essentially final and conclusive civil or commercial monetary judgments from designated Mainland courts), important prerequisites being an exclusive jurisdiction clause providing for the Mainland courts and an application for registration within two years. An updated arrangement was signed in January 2019 extending the scope of reciprocal enforcement (to remove the requirement of an exclusive jurisdiction clause and also cover non-monetary relief, but excluding certain IP matters), but has yet to come into operation. The Mainland Judgments in Civil and Commercial Matters (Reciprocal Enforcement) Bill (to implement the arrangement locally) was introduced to the local Legislative Council in early 2022. Hong Kong is a party to the New York Convention through China. Hong Kong arbitral awards are enforceable in other New York Convention countries and vice versa.
China	Court orders can be enforced by the court of first instance or the court at the same level where the property subject to execution is located. A foreign judgment is generally not enforceable in China unless otherwise specified or agreed in a bilateral treaty or convention. A foreign arbitration award is enforceable in China under the New York Convention and vice versa.

Jurisdiction	Consideration
Singapore	With respect to Singapore court proceedings, compliance with court orders can be enforced through contempt proceedings with the possibility of imprisonment for anyone involved. Foreign court judgments are not automatically enforceable in Singapore as if they were judgments of the Singapore court. Where a treaty provides for reciprocal recognition and enforcement of judgments between Singapore and a foreign country, an application can be made to register the foreign court judgment in the Singapore court pursuant to the treaty. Singapore is a signatory to the New York Convention. Singapore arbitral awards are therefore enforceable in other New York Convention countries and vice versa
Japan	Japan is a signatory to the New York Convention. Therefore, foreign arbitral awards issued in countries that are also signatory states to the New York Convention are recognised and enforced in Japan in accordance with the direct application of the New York Convention, unless there is any other relevant bilateral treaty which prevails over the application of the New York Convention. Other foreign arbitral awards are recognised and enforced in Japan in accordance with the Arbitration Act, which is a local law governing the recognition and enforcement of arbitral awards (domestic and foreign arbitral awards) in Japan. The language of the provisions regarding the recognition and enforcement of arbitral awards in the New York Convention and the Arbitration Act is not identical, but it is generally considered that there is no substantial difference in the consequences with respect to recognition and enforcement based on the application of the provisions. Broadly consistent with the UNCITRAL Model Law on which it is based, the Arbitration Act provides that, subject to where certain grounds for refusing enforcement exist (discussed further below), an arbitral award (domestic or foreign) has the same effect as a final and conclusive judgment of a Japanese court. However, arbitral awards (domestic and foreign) require an execution order to be made by a competent court in Japan to be enforceable in Japan. Article 44 of the Arbitration Act contains grounds for setting aside an arbitral award that are substantially the same as those contained in the UNCITRAL Model Law. Article 45 of the Arbitration Law contains grounds for refusing to enforce an arbitral award that are substantially the same as those contained in the UNCITRAL Model Law and the New York Convention. A foreign judgment must satisfy a number of requirements in order for an execution order to be obtained from a competent court in Japan for its enforcement in Japan. These requirements include (i) the foreign judgment must be final and conclusive; (ii) the service of process was effected other than by public notice or some other similar method, or the counterparty has appeared in the relevant proceedings in the foreign jurisdiction; (iii) judgments of Japanese courts receive reciprocal treatment in the courts of the foreign jurisdiction concerned; (iv) the foreign judgment (including the court procedures leading to such judgment) is not contrary to public order or the good morals doctrine in Japan; and (v) the dispute resolved by the foreign judgment has not been resolved by a judgment given by a Japanese court and is not being litigated before a Japanese court.

Jurisdiction	Consideration
Australia	Australian courts are reliable and effective in enforcing judgments and arbitral awards as corruption is extremely low and failure to comply with a court's order may result in an order finding a recalcitrant party in contempt. Domestic judgments are enforceable by the court in which the judgment was made, or where the judgment is interstate, by registering the judgment with the Federal Court or Supreme Court in the State or Territory in which enforcement is sought. Enforcement of foreign judgments and arbitral awards may be made pursuant to the Foreign Judgments Act 1991 (Cth) and related regulations. Further, international arbitral awards may be enforced by Australian courts under the International Arbitration Act 1974 (Cth). Australia is a signatory to the New York Convention. Australian arbitral awards are enforceable in other New York Convention countries and vice versa.

(f) Requirement for emergency or interlocutory relief

Jurisdiction	Consideration
Hong Kong	Hong Kong courts will generally grant interim relief in aid of Hong Kong-seated or foreign arbitrations and Hong Kong or foreign court proceedings. For arbitration proceedings interim relief is available from the court and in many cases from emergency arbitral panels. Hong Kong courts will also enforce interim and emergency awards issued by an arbitral tribunal. In April 2019, Hong Kong and Mainland China entered into a mutual arrangement making it possible to seek interim relief from the Chinese courts in aid of Hong Kong-seated arbitrations administered by mutually acknowledged institutions, including the HKIAC, CIETAC HK and ICC Asia Office. The arrangement is significant for making Hong Kong the first (and, to date, only) seat of arbitration outside Mainland China where parties can access the Mainland court system for interim measures in aid of offshore arbitration. This is relevant to those contracting with Mainland Chinese parties or dealing with assets or projects in Mainland China. The Supreme People's Court Notice implementing the arrangement in Mainland China took effect on 1 October 2019.
China	While interim injunctions and preservation of evidence or property are theoretically available from PRC courts, they are difficult to obtain in practice. A domestic arbitral tribunal does not have any power to grant interim relief or interim awards. Such matters have to be referred to the PRC court.
Singapore	Emergency and interlocutory relief is generally available for Singapore court proceedings and Singapore-seated arbitrations. Singapore courts will generally grant interim relief in aid of domestic and foreign arbitration. Singapore courts will also enforce interim and emergency awards issued by an arbitral tribunal.
Japan	Interim measures are generally available for both court proceedings and arbitrations seated in Japan. However, interim measures ordered by the arbitral tribunal are not enforceable (unlike those ordered in the context of court proceedings) unless a local court makes orders in support of the arbitral tribunal's orders.

Jurisdiction	Consideration
Australia	The court will grant an interim injunction when it believes there is a serious question to be tried, that monetary damages will not be an adequate remedy and where the balance of convenience favours the granting of an injunction. These orders are usually for brief periods of time (one or two days) following which the court will assess whether the injunction should continue. Compensation may be awarded if it is later found that the interim injunction should not have been ordered. Interim measures can be granted by an arbitral tribunal in order to maintain or preserve the status quo, take action to prevent imminent harm, preserve assets or preserve evidence.

(g) Discovery requirements

Jurisdiction	Consideration
Hong Kong	Discovery in court proceedings requires parties to disclose all documents relevant to the issues of the case. These will include documents which may damage a party's own case. Since arbitration procedures are more flexible, the parties or the arbitral tribunal may set discovery requirements different from those in court proceedings to save costs and time. For example, disclosure can be limited to certain types or categories of documents, or the parties can choose to disclose documents at different stages including at the pleading stage.
China	China does not have an evidence discovery procedure as distinguished from evidence exchange. In practice, it is not easy for a plaintiff to provide evidence of an alleged infringing act, especially when such information is not publicly available. One exception is that the defendant bears the burden of proof when a product manufactured by a patented process is a new product; in this case, an infringer has the burden of proving that the manufacturing process they have used is different from the process that is claimed to have been patented. Where it is likely that evidence may be destroyed, lost or become difficult to obtain later on, a party may apply to a PRC court for the preservation of the evidence. According to CIETAC rules, a party bears the burden of proof for its claims and counterclaims and may suffer adverse consequences if it fails to provide such evidence in a timely fashion.
Singapore	The obligation to disclose documents in arbitration is generally considered narrower than in court proceedings in Singapore. For example, it is generally accepted that commercial confidentiality may be a basis for non-disclosure in arbitration proceedings. That is not the case for court proceedings where a relevant document has to be disclosed unless it is privileged. Furthermore, pre-arbitration discovery is not within the jurisdiction of the Singapore courts to order.
Japan	Japan is a civil law jurisdiction and, like other such jurisdictions, document disclosure in civil court proceedings is generally very limited. The obligation to disclose documents under Japan's Code of Civil Procedure (Act No. 109 of 1996, as amended) contains a series of exceptions, including one in relation to confidential documents that were created solely for the use of the holder. Under Japanese law, parties are free to agree documentary discovery procedures for their arbitration. However, in the absence of such an agreement, should the assistance of a Japanese court be sought for the production of documents, the court will be obliged to observe the same series of exceptions mentioned above when making an order for disclosure. Disclosure will consequently be more limited than in common law countries.

Jurisdiction	Consideration
Australia	Discovery in court proceedings requires parties to provide lists of, and disclose, all documents relevant to the issues of the case. These will include documents which may damage a party's own case. However, the parties may apply for a confidentiality regime to protect inadvertent public disclosure of commercially sensitive information. Since arbitration procedures are more flexible, the parties or the arbitrator may set discovery requirements different from those in court proceedings to save costs and time. For example, lists of documents can be limited to certain types or categories of Documents, or the documents themselves may be allowed to be attached and disclosed at different stages, such as at the pleading stage.

2.12 Standard Essential Patents and FRAND arbitration

Regulators around the world have recently shown greater willingness to encourage arbitration or ADR as a form of dispute resolution for FRAND-related disputes which invariably involve issues on the proper level of royalties for SEPs. It would seem that the reasoning behind this policy is that both parties benefit from this mechanism. The licensor obtains a contractual commitment from the licensee to pay royalties (with the level of royalties being determined objectively by a neutral tribunal), while the licensee does not face any risk that the threat or the issuance of an injunction will compel it to accept a royalty that is greater than FRAND.

SEP disputes can be complicated, and the parties may not always have a contract or may be unable to agree to resolve the dispute through arbitration. In the absence of any agreement – and faced with a patent infringement claim – it does not seem realistic to expect the parties to be able to agree on arbitration when there may be a multitude of other disputed issues including the scope of patent claims, the relevant standards, the products in issue, the jurisdictions and the term. On the other hand, where the only issue in dispute is with respect to the appropriate royalty rate, arbitration may be an attractive and useful means of resolving the dispute.

2.13 Smart Contracts

Smart contracts often use blockchain technology to record and execute transactions. **See Section 1.14**.

Smart contracts also often involve an entirely blockchain-enabled organisation, otherwise known as a decentralised autonomous organisation (DAO), which operates through preprogrammed smart contracts without human involvement. DAOs have no legal personality. In the event of any defect in the blockchain process or the trade or the code of the smart contract, the question arises whether it is the DAO or the blockchain operator or even the coder (given that smart contracts are essentially prewritten computer codes) that will be liable for any damage caused by the defect. There is also the question whether and how the smart contract could be frustrated or made void under traditional contract principles, such as "mistake", which may occur in the course of executing the smart contract.

For further information on Smart Contracts, please see our briefing **Considerations Around Smart Contracts: Contracts Between Computer Programs**

ENFORCEMENT OF RIGHTS

3. ENFORCEMENT OF RIGHTS

IP rights are meaningless unless they can be enforced. IP rights can act both as a shield, such as in defending against infringement claims, and as a sword, for example by protecting a right against unauthorised use. IP enforcement is also used as leverage to obtain cross-licence arrangements, especially in industries where a variety of IP or inventions is needed to produce a product.

3.1 How can I best enforce my technology rights?

This depends on the jurisdiction, who the technology rights are being enforced against, and whether the rights stem from an underlying contract.

A useful framework for determining how best to enforce technology rights is as follows:

(a) What right is sought to be protected?

i. The starting point is to determine the precise right that is sought to be protected and the relief that is ultimately desired.

ii. This helps narrow down the possible causes of action that might subsist and has a material bearing on the jurisdiction in which the rights are sought to be asserted since certain rights may not be enforceable in all jurisdictions.

(b) Where do I want to assert the right?

i. The choice of forum may have a bearing on the type of remedies available as a matter of course.

ii. It may also be useful to consider the attitudes that the various jurisdictions under consideration have previously adopted towards similar claims or claims premised on similar rights.

(c) Who am I enforcing my right against?

i. If there is no contractual relationship between the parties, that may affect the ability to obtain certain types of relief.

ii. The presence or absence of a contractual relationship may also limit the available dispute resolution possibilities.

MODES OF DISPUTE RESOLUTION FOR TECHNOLOGY DISPUTES			
	Court Proceedings	**Arbitration**	**Mediation**
Parties' Agreement	No agreement between parties needed	Parties need to agree to arbitration	Parties need to agree to ADR
Interim and Emergency Relief	Available	Available	Not applicable
Timing	Procedures could be drawn out	Arbitrator(s) and parties can shorten the procedure	Mediator(s) and parties can shorten the procedure
Costs	Can be costly due to inflexibility in procedure; for example, discovery	Costs can be reduced through flexibility in procedure, but additional costs such as for tribunal and hearing facilities	Typically less than court proceedings or arbitration
Possibility of Appeal	Possible to appeal to higher courts	Generally, no right to appeal, but limited grounds for setting aside and resisting enforcement	None, outside of any contractual challenge of a documented agreement
Adjudicator	Some courts have lists of technology specialists. Otherwise, the decision-maker may not be a specialist in the subject matter.	Parties can select arbitrator(s) with relevant expertise	Parties can select mediator(s) with relevant expertise
Confidentiality	Public proceeding	Private and confidential procedure	Private and confidential procedure
International Enforcement	The Hague Convention on Foreign Judgments in Civil and Commercial Matters entered into by one nation allows for enforcement of its judgments by legal authorities in other signatory nations Risk of multiple proceedings under different laws, with risk of conflicting results Possibility of actual or perceived home court advantage of the party that litigates in its own country	A single proceeding under the law determined by the parties Arbitral procedure and nationality of arbitrator can be neutral with respect to law, language and institutional culture of the parties The New York Convention allows for enforcement of arbitral awards in many jurisdictions	

Special arrangements for enforcement as between China and Hong Kong

As Hong Kong is a special administrative region of China, the two are not separate countries and international conventions cannot be relied upon for reciprocal enforcement. Special arrangements between the two jurisdictions must be reached. A 2019 arrangement enables Mainland court judgments to be enforced in Hong Kong (and vice versa, subject to conditions) by way of a simple registration procedure. In terms of the impact on IP disputes, this will facilitate enforcement of court judgments issued in IP contractual disputes and monetary damages awarded in IP infringement disputes. In November 2022, Hong Kong passed legislation to prepare for implementation of the said arrangement in about six to seven months' time. For a discussion of the practical effects of the arrangement and Hong Kong legislation, see out Global IP Update article **Hong Kong passes legislation to implement latest arrangement with Mainland for reciprocal enforcement of civil and commercial court judgments – impact on IP disputes**.

3.2 Where an infringement of IP has been established, what relief is available?

Where an infringement of IP has been established, the relief which may be available includes injunctions, damages and account of profits.

Jurisdiction	Judicial	Administrative/Criminal	Breach of contract
Hong Kong	A Hong Kong court can make any of the following orders: 1. injunction; 2. delivery up and/or destruction of the infringing items; 3. disclosure order to reveal the source of the infringing items; and 4. damages or account of profits.	The Customs and Excise Department of the Government of the Hong Kong SAR is the enforcement agency in Hong Kong responsible for criminal enforcement of trademark and copyright infringement. The Department investigates complaints alleging trademark and copyright infringement as well as complaints alleging false trade descriptions. It also has extensive powers of search and seizure. **Copyright:** A person who commits copyright piracy, such as making for sale or hire an infringing copy, is liable on conviction on indictment to a fine of HK$50,000 per infringing copy and to imprisonment for four years. A person who makes or possesses equipment for copyright piracy is also liable on conviction on indictment to a fine of HK$500,000 and to imprisonment for eight years. Where an effective technological measure has been applied in relation to a copyright work in order to protect the same, a person who makes circumvention devices or provides commercial services for enabling customers to defeat such measures is liable to a fine of HK$500,000 and to imprisonment for four years. **Trademark:** A person who forges or falsely applies any trademark commits an offence under the Trade Descriptions Ordinance (Cap. 362) and is liable on conviction on indictment to a fine of HK$500,000 and to imprisonment for five years.	An injured party can seek to enforce its rights in accordance with the contractual dispute resolution mechanism chosen, whether it be court proceedings, arbitration, mediation or negotiation. Contracts will often include provisions on the type, calculation and extent of damages and legal costs. To the extent that the contract provides for damages or costs, those provisions may be relevant in determining the type of relief available. Appropriate indemnity clauses would assist, if included.

Jurisdiction	Judicial	Administrative/Criminal	Breach of contract
China	The PRC court can make any of the following orders: 1. injunction; 2. damages or statutory damages; and 3. elimination of any adverse effects.	The PRC administrative authorities can generally take one of the following actions in respect of an IP infringing act: 1. order to cease the concerned infringing act; 2. confiscation of illegal gains; 3. seizure of infringing goods; and 4. fines. The criminal liabilities of IP infringement-related crimes, such as trademark or copyright infringement and trade secret misappropriation, include: 1. fines with an amount to be decided by a court based on the severity of an infringing act; and/or 2. fixed term imprisonment or criminal detention for a maximum term of 10 years.	An injured party can seek to enforce its rights in accordance with the contractual dispute resolution mechanism chosen, whether it be court proceedings, arbitration, mediation or negotiation. To the extent that the contract provides for damages or loss suffered, those provisions may be relevant in determining the type of relief available. The non-defaulting party may generally seek an order of compensation for damages, corrective actions or specific performance from a PRC court or arbitral tribunal.
Singapore	The remedies which a Singapore court can order to address an IP infringement include: 1. injunction; 2. damages or an account of profits; 3. an order for delivery up and/or disposal of the relevant infringing item	In addition to civil proceedings, an injured party may enforce its rights in criminal proceedings. Examples of infringing activities giving rise to criminal liability include counterfeiting a registered trademark and importing or selling goods with a falsely applied trademark. Conviction for such offences attracts severe penalties: a fine of up to S$100,000 and/or imprisonment for a maximum term of five years. Singapore courts take a very serious view of trademark offences; custodial sentences are the norm unless the quantity of infringing articles is quite small. The imposition of strong deterrent sentences is part of the efforts to promote Singapore as a regional intellectual property centre and the concomitant need to clamp down on piracy of intellectual property.	An injured party can seek to enforce its rights in accordance with the contractual dispute resolution mechanism chosen, whether it be court proceedings, arbitration, mediation or negotiation. To the extent that the contract provides for damages or loss suffered, those provisions may be relevant in determining the type of relief available.

Jurisdiction	Judicial	Administrative/Criminal	Breach of contract
Japan	Relief for infringement of IP rights includes (a) injunction and/or (b) compensation for damages.	Japanese Customs has an injunction system to prevent the importation of products infringing the following IP rights: 1. Patent Rights 2. Utility Model Rights 3. Design Rights 4. Trademark Rights 5. Copyright 6. Plant Breeder Rights and 7. Interests protected under the Unfair Competition Prevention Act (UCPA) There is no minimum threshold below which the infringements set out below are considered criminal in nature. If any infringing activity occurs (e.g., production of infringing products), such activity constitutes a criminal act. However, the relevant prosecutorial authority has full discretion with respect to the decision to prosecute. In other words, if the damage to the IP owner is insignificant, the Prosecutor would likely not lay criminal charges. **Trademark infringement:** Imprisonment of not more than 10 years and/or penalty of not more than ¥10 million (Article 78 of the Trademark Act (Act No. 121 of 1959, as amended)). **Trade secret infringement:** Imprisonment of not more than 10 years and/or penalty of not more than ¥20 million (Article 21 of the Unfair Competition Prevention Act). **Copyright infringement:** Imprisonment of not more than 10 years and/or penalty of not more than ¥10 million (Article 119 of the Copyright Act (Act No. 48 of 1970, as amended)).	An injured party can seek to enforce its rights in accordance with the contractual dispute resolution mechanism chosen, whether it be court proceedings, arbitration, mediation or negotiation. To the extent that the contract provides for damages or loss suffered, those provisions may be relevant in determining the relief available. The relevant court or arbitral tribunal may award an injunction and/or compensation for damages.

Jurisdiction	Judicial	Administrative/Criminal	Breach of contract
Australia	The court may grant final injunctions, damages and/or an account of profits to compensate the IP owner for the infringements.	**Patents:** For all offences under the Patents Act 1990, Chapter 2 (general principles of criminal responsibility) of the Criminal Code Act 1995 applies. There is a long list of offences which carry a financial penalty and one offence which carries a penalty of imprisonment. Penalty amounts vary according to the particular infringement. **Copyright:** Penalties for offences range from purely financial to imprisonment. For any penalty listed under the Act, a body corporate can receive up to five times the punishment compared with the penalties where only an individual person is identified. The Copyright Act also sets out indictable offences (a penalty of either financial or imprisonment, or both). Some of these offences can alternatively be charged as summary offences or strict liability offences in certain circumstances. Penalty amounts vary according to the infringement concerned. **Trademark infringements:** For all offences under the Trademarks Act 1995, Chapter 2 (general principles of criminal responsibility) of the Criminal Code Act 1995 applies. For any penalty listed under the Act, a body corporate can receive up to five times the punishment where only penalties for an individual person are identified. Penalties include imprisonment or financial penalties (or both) and offences include indictable offences, which can alternatively be charged as summary offences in certain circumstances. Certain offences carry only a financial penalty. The amount of the penalty varies according to the particular infringement.	An injured party can seek to enforce its rights in accordance with the contractual dispute resolution mechanism chosen, whether it be court proceedings, arbitration, mediation or negotiation. To the extent that the contract provides for damages or loss suffered, those provisions may be relevant in determining the type of relief available. Contracts will often include provisions on the type, calculation and extent of damages and legal costs which can be awarded. Appropriate indemnity clauses will assist, if included. Aside from IP law, there are other avenues that can be taken to protect technology and IP interests. For example: **Misleading and deceptive conduct:** Under the Australian Consumer Law (Cth) a civil proceeding can be brought where there has been misleading or deceptive conduct. This may occur where a company purports to have certain features in a product which are covered by IP rights, when in fact it does not have those features. Misleading and deceptive conduct may be proven even where there is no breach of IP rights. **Breach of confidentiality:** This common law cause of action can be brought against a person who intends to breach, or has breached, a duty of confidence by disclosing protected information.

3.3 What interim or quick relief is available against wrongful users of technology or IP?

Jurisdiction	
Hong Kong	Injunctions or emergency relief may be obtained from the courts or arbitral tribunals. Some companies also co-operate with Hong Kong Customs on a regular basis on inspections, raids, and seize and search operations for products which infringe their technology or intellectual property rights.
China	Interim injunctive relief is available from courts for certain types of IP infringements. Orders for pre-action or pretrial asset and evidence preservation may also be obtained subject to the payment of security. Administrative enforcement may be an alternative way to stop infringement quickly as administrative authorities can often take enforcement actions rapidly. However, administrative decisions may be appealed and any orders made will be stayed pending appeal.
Singapore	An interim injunction may be taken out to restrain the infringing party from continuing its wrongful use of or violation of the technology or intellectual property right.
Japan	A provisional injunction order under the Civil Provisional Remedies Act (Act No. 91 of 1989, as amended) is available before starting judicial or arbitration proceedings. In proceedings seeking a provisional injunction order, the level of proof of infringement is less than that of normal judicial proceedings, but "urgency" for the protection of the IP rights in question is required.
Australia	Interim relief can be achieved through interlocutory injunctions made to the court. It should be noted that these orders are usually very brief (one to two days) and the court will then reassess whether the injunction should continue. An applicant seeking interlocutory relief must provide an undertaking as to damages. If, at the end of a proceeding, the court finds that the interlocutory injunction should not have been made, an order for compensation may be made against the applicant.

3.4 Can electronic evidence and computer output be admitted as evidence? Are electronic signatures admissible as evidence and do they have the same effect as if documents were signed by hand?

Jurisdiction	
Hong Kong	According to section 9 of the Electronic Transactions Ordinance (ETO), an electronic record cannot be denied admissibility as evidence in any legal proceedings on the sole ground that it is an electronic record without prejudice to any rules of evidence. On 17 July 2020, the Court Proceedings (Electronic Technology) Ordinance (Cap 638) was passed and came into effect on 1 October 2021. It makes provision for electronic service and filing of court documents, recognition of electronic signing and authentication of court-related documents, electronic document production and electronic payment. In association with this development, the Judiciary has been working on an Integrated Court Case Management System to facilitate electronic court processes. This will be implemented in phases; firstly, with respect to District Court civil cases, then criminal cases and other courts, including the High Court and Court of Final Appeal, with a final phase for all other remaining courts. The phased implementation commenced on 1 October 2021 on a voluntary basis. Despite the gradual process of these reforms – due to the impact of COVID-19 – the use of technology in Hong Kong courts has otherwise increased to some extent, including allowing certain hearings to be conducted remotely by telephone or videoconference, as well as use of online data rooms for electronic service of certain court documents and the choice of electronic document production for compliance with disclosure orders made in certain circumstances. E-signatures are recognised under Hong Kong law. The use of electronic signatures is governed by the ETO. For transactions where all parties are non-governmental entities, signatories can agree to use electronic signatures or digital signatures. For transactions that involve government entities, signatories must use digital signatures (supported by a recognised certificate issued by a certification authority). Hong Kong law recognises electronic signatures for the purpose of most contracts. However, there are certain exceptions that require handwritten signatures under Schedule 1 of the ETO, such as testamentary documents, certain trust documentation, documents concerning land and property transactions, and powers of attorney. An electronic signature is valid where: 1. the signatory attaches his or her electronic signature to, or associates it with, an electronic record for the purpose of identifying himself or herself and indicating authentication or approval of the information in the electronic record; 2. the method used by the signatory is reliable, and appropriate, for the purpose for which the information contained in the document is communicated; and 3. the person to whom the signature is given consents to the use of such method.

Jurisdiction	
China	The PRC Electronic Signature Law recognises the legal effect of an e-signature and electronic data. The admissibility of electronic data and evidence cannot be denied merely because they are in electronic format. Any electronic data that can show, in material form, the contents that it specifies, and which may be accessed and used at any time, is regarded as complying with the written format as prescribed by laws and regulations. Electronic data or evidence includes emails, web pages, short messages, faxes, etc. A reliable e-signature has the same legal effect as if the document were signed by hand. An e-signature is regarded as a reliable electronic signature if it satisfies the following conditions: 1. the data made by electronic signature is used for the electronic signature, and is owned exclusively by the electronic signatory; 2. the data made by electronic signature is controlled only by the electronic signatory, at the time of signing; 3. it is possible to ascertain whether any alteration has been made to the electronic signature, after signature; and 4. it is possible to ascertain whether any alteration has been made to the content and form of any electronic data after signature. The parties may also choose to use an electronic signature which complies with their chosen stipulations.
Singapore	In Singapore, the admissibility of evidence is governed by the Evidence Act. The definition of "evidence" is broad enough to encompass information recorded in an electronic medium or recording device, such as a hard disk drive installed in a computer or server. Thus, a document in electronic form constitutes evidence under the Evidence Act. Under the Singapore Electronic Transactions Act, an electronic signature has the same legal status as a physical signature. Where a rule or law requires a signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law. Where the authenticity of a computer output is challenged, the authenticity of the electronic signature may become an issue. An electronic signature may be proved in any manner, including by showing that a procedure exists requiring a transacting party to undergo a verification procedure.
Japan	Electronic data (including, without limitation, data stored on a computer or server, audio recordings, and video materials) can be admitted as evidence. However, the party who submits such evidence is required, at the request of the court or the opposing party, to submit a document explaining its contents. It is also permissible (and common) to submit a transcription or hard copy output or printout of electronic data as evidence, in lieu of the electronic data itself. In such cases, the party who submits the transcription or output is required, at the request of the opposing party, to deliver a copy of the underlying electronic data to that party. Electronic signatures are admissible as evidence, but (naturally) they must be authentic in order to be afforded an evidentiary weight. The Electronic Signatures and Certification Business Act (Act No. 102 of 2000, as amended) (the ESA Act) sets out various requirements in order for electronic signatures to be deemed authentic. The weight afforded to electronic as opposed to documentary or quasi-documentary evidence (whether certified or not) will be determined according to the free evaluation principle, offering a significant amount of discretion to the Court (in this regard, refer to Article 247 of the Code of Civil Procedure (Act No. 109 of 1996, as amended)).

Jurisdiction	
Australia	The "original document rule" no longer applies in Australia, allowing for a copy of a document to be produced by a device (e.g., photocopier or computer) which reproduces the contents of documents as well as digital extracts of business records. It may be necessary to give evidence that the digital record is what it purports to be. Metadata (information that is associated with, or embedded in, a document) is considered as part of the document. Procedures are now in place that allow for the authenticity testing of evidence. These include orders which may demand that the original document be produced, that the other party be permitted to examine, test or copy the document, or that the other party be permitted to examine and test the method by which a document was produced or has been kept. The Electronic Transactions Act 1999 (Cth) allows that where information is in writing, a signature or retaining information is required under a law of the Commonwealth; these requirements can be met by electronic means unless specifically excluded in Commonwealth legislation (e.g., Statutory Declarations). Electronic signatures can be made in a variety of ways: a name typed on a document, a scanned manuscript signature, a signature captured by a digital pen on accompanying software, and digital signatures. Personal Identification Numbers (PINs) and passwords may also be classified as electronic signatures. Electronic signatures are treated the same as handwritten signatures, subject to the following conditions: 1. The recipient has consented to receive information electronically. 2. The method of signing identifies the person sending the information and indicates they approve of the content of the electronically signed document. 3. The method of signing must be as reliable as appropriate for the purposes of the document, with regard to the circumstances of the transaction (for example, contracts for sale of land will not allow electronic signatures).

3.5 Is there any way I can consolidate multijurisdiction technology disputes in one forum?

This depends on the nature of the dispute and the parties involved. If an arbitration agreement applies to the disputes, it may be possible to have the disputes resolved by arbitration in a single forum. For example, under the WIPO Arbitration Rules, it is possible to consolidate IP disputes into a single arbitral proceeding.

3.6 What are the options to appeal against a judgment or an award?

Jurisdiction	Arbitration	Judicial
Hong Kong	The arbitral tribunal's award is final and binding, although an appeal to the court on a question of law can be made if the arbitration agreement falls within one of those types or in the circumstances set out in sections 99 to 101 of the Arbitration Ordinance, including the parties expressly opting in. Apart from an appeal, the only other active recourse against an arbitral award is an application to the Court to set it aside, pursuant to section 81 of the Arbitration Ordinance. The Arbitration Ordinance sets out the limited circumstances in which an arbitral award may be set aside by the court, namely: 1. incapacity of a party; 2. invalidity of the arbitration agreement; 3. a party has not been given proper notice of the appointment of an arbitrator or the arbitral proceedings or is otherwise unable to present his or her case; 4. the award dealing with a dispute not falling within the terms or scope of the submission to arbitration; 5. the composition of the arbitral tribunal or the arbitral procedure not being in accordance with the parties' agreement or Hong Kong law; 6. the subject matter of the dispute not being capable of settlement by arbitration under Hong Kong law; or 7. the award being in conflict with Hong Kong's public policy.	An individual may sue another for infringement of any intellectual property rights by commencing a civil action in the court. There are a number of courts in Hong Kong that deal with civil actions, such as the Small Claims Tribunal, the District Court and the High Court (which comprises the Court of First Instance and Court of Appeal). The court in which a civil action should be brought depends on the type of the relief sought, the amount of money claimed, etc. An Intellectual Property Specialist List in the Court of First Instance was created in May 2019. All interlocutory applications and trials in intellectual property cases are now listed before the judge in charge of the list or other designated judges, the purpose of which is to enhance case management and reduce costs and delay. Court of First Instance – The Court of First Instance hears appeals from Magistrates' Courts and the Small Claims Tribunal Court of Appeal – The Court of Appeal hears appeals on all civil and criminal matters from the Court of First Instance and the District Court Court of Final Appeal – The Court of Final Appeal hears appeals on civil and criminal matters from the High Court

Jurisdiction	Arbitration	Judicial
China	Pursuant to the PRC Arbitration Law, an arbitral award is final and binding on the parties. After an arbitral award is rendered, a PRC court or an arbitration commission will refuse to entertain applications for arbitration or legal proceedings in respect of the same dispute. If the arbitration award is set aside or is not enforced by a PRC court, the parties may apply for arbitration or initiate legal proceedings with the PRC court.	An appeal may be filed against a ruling of a court on matters such as refusal to entertain a case, objection to the jurisdiction of a court and dismissal of a complaint. If a party disagrees with a first instance judgment made by a local court, the party has the right to lodge an appeal with the immediate superior court within 15 days from the date on which the written judgment was served. The judgments and rulings of the court of second instance are considered final. Any party that considers a legally effective judgment or ruling to be wrong may apply to the immediate superior court for retrial. Where a case involves a party comprising a large number of individuals, or if both parties are individuals, the parties may apply to the original court for a retrial of the case. The application for retrial does not mean that the enforcement of the judgment or ruling is suspended.
Singapore	Arbitral awards may be set aside on very limited grounds as provided by Article 34 of the UNCITRAL Model Law on International Commercial Arbitration and s 24 of the International Arbitration Act. One example of a basis for setting aside an arbitral award is if the award deals with a dispute not contemplated by, or not falling within the terms of, the submission to arbitration, or if it contains decisions on matters beyond the scope of the submission to arbitration. There are also means to challenge the enforcement of an award.	In Singapore, high court judgments are generally appealable as of right to the Singapore Court of Appeal. The aggrieved party may appeal on the basis that the High Court judge was wrong on the law or even on the facts.

Jurisdiction	Arbitration	Judicial
Japan	Arbitral awards are final and binding and may not be appealed in court. In order to enforce an arbitral award, it is necessary to obtain an enforcement order from the court. However, if any of the following scenarios apply, then, pursuant to Articles 44 and 45 of the Arbitration Act, the arbitral award may either be set aside or not enforced: 1. the arbitration agreement is held not to be valid because a party lacked the requisite capacity to enter into the agreement; 2. the arbitration agreement is held not to be valid under the governing law of the agreement (or, in the absence of any such provision in the agreement, the laws of the place of arbitration); 3. a party was not given the requisite notice when appointing arbitrators or during the arbitral procedure, to the extent required by the laws of the place of arbitration (or such legal notice requirements otherwise agreed between the parties); 4. a petitioner was impeded from presenting its defence in the arbitral proceedings; 5. the arbitral award concerns decisions relating to matters outside the scope of the arbitration agreement or the claims in the arbitral proceedings; 6. the composition of the arbitral tribunal or the arbitral proceedings were not in accordance with the laws of the place of arbitration (or such legal composition/procedural requirements otherwise agreed between the parties); 7. according to the laws of the country (place) of the arbitration (or, if the parties have agreed that the law of a different country governs the arbitration, the laws of that country), the arbitral award has not yet become binding, or the arbitral award has been set aside or suspended by a court of such country; 8. the claims in the arbitral proceedings relate to a dispute that, by operation of Japanese law, is not arbitrable; or 9. the content of the arbitral award is contrary to Japanese public policy.	The Tokyo District Court and the Osaka District Court are courts of first instance, each possessing specialist divisions with exclusive jurisdiction to deal with intellectual property disputes. The Intellectual Property High Court hears appeals against judgments issued by these Courts. For IP disputes relating to matters other than those set out above, each High Court registry in Japan has jurisdiction and will hear appeals against judgments issued by any District Court in Japan. The Supreme Court of Japan stands as the court of final appeal against judgments issued by the High Court or the IP High Court. In relation to arbitral awards, subject to the grounds for setting aside or resisting enforcement provided for in the Arbitration Act (see above), foreign and domestic arbitral awards are not subject to a merits review/appeal mechanism.

Jurisdiction	Arbitration	Judicial
Australia	In international arbitration, an award is binding on a party to the investment dispute to which the award relates and the award is not subject to any appeal or other remedy, unless in accordance with the Convention on the Settlement of Investment Disputes, which allows matters of interpretation, revision or annulment of the award to be examined in limited circumstances. In domestic commercial arbitrations, appeals to courts against arbitral awards are permitted if they are appeals relating to a question of law, and only if the parties agree within a set period of time that an appeal may be made and the Court grants leave. Leave will be granted, if it was a question the tribunal was asked to determine, where the determination will substantially affect the rights of one or more of the parties, or if on the basis of the findings of fact, where the decision is obviously wrong or open to serious doubt and it is just and proper for the Court to determine the question.	Proceedings are commenced in either the Supreme Court of the relevant State or Territory, or, more commonly for IP-related disputes, the Federal Court. An appeal from a decision of a Supreme Court or Federal Court judge may be made to the relevant Court of Appeal. Leave may be required before an appeal can be heard. Appeals are often only permitted on a point of law. Court of Appeal decisions can be appealed, subject to leave being granted, to the High Court. The High Court's judgment is final and there are no more avenues of appeal from that Court.

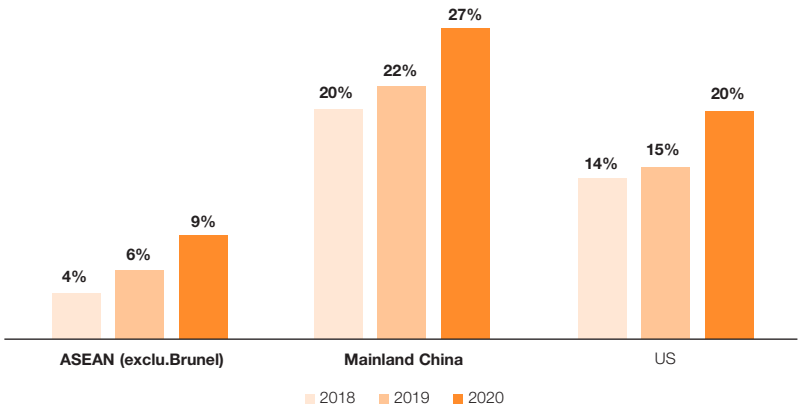
E-COMMERCE AND RETAIL DIGITAL PLATFORMS

4. E-COMMERCE AND RETAIL DIGITAL PLATFORMS

COVID-19 has put a strain on traditional retail, given lockdown and social distancing measures leading to closure of physical stores. On the other hand, the shift towards online retail channels has accelerated. The value of ASEAN's e-commerce has expanded almost sixfold in just four years, increasing from US$9.5 billion in 2016 to US$54.2 billion in 2020. E-commerce sales as a percentage of total sales hit 9% in 2020, up from 4% in 2018. The room for growth can be illustrated by how these figures still fall behind Mainland China and the US, where e-commerce accounted for 27% and 20% of total sales in 2020, respectively.[5]

E-commerce Share

E-commerce sales as percentage of totlal retail sales



Source: Euromonitor Passport database

The legal framework governing e-commerce in APAC countries is generally based on a combination of consumer protection (such as protecting against false advertising and unconscionable contracts, as well as providing for quality and safety); intellectual property protection; data protection and privacy; and banking and payment system laws. Some countries have additionally codified specific legislation covering electronic communications and transactions and some have specific e-commerce legislation. For example, Hong Kong has an Electronic Transactions Ordinance, which governs digital and electronic signatures and contracts, as well as an Unsolicited Electronic Messages Ordinance, which regulates such messages for advertisement and promotion sent by electronic media and requires specific information to be accurate and the inclusion of an unsubscribe facility. China has a specific E-Commerce Law, which came into force on 1 January 2019 covering platform operators, vendors operating on third party platforms, and those operating through their own websites or other network services, such as social media. The focus is on consumer protection through transparency and intellectual property rights protection. It deals with the registration and licensing of e-commerce operators and the requirement to display the same; false advertising; product and service safety; electronic contracts and payment; data

5 HKTDC Research, ASEAN E-commerce: Beyond the Pandemic, 9 June 2021, https://research.hktdc.com/en/article/NzY4MzkzMzg1

protection; cybersecurity; imposition of joint liability between vendors and platform operators if the latter do not take necessary measures; notice and take-down procedures in relation to intellectual property rights infringement; and dispute resolution (including a requirement to establish an effective complaints mechanism).

Platform operators potentially face liability in instances of violations of intellectual property and data privacy rights. However, in most jurisdictions, they have the benefit of exemptions based on their position as intermediaries and particularly where they do not have knowledge of the unlawful activity. On the other hand, if the unlawful activity is not addressed upon becoming aware of the same, secondary liability may be imposed. In China, as mentioned above, the E-Commerce Law makes provision for intellectual property rights owners to give notice of infringement and for platform operators (and vendors) to respond and otherwise take measures such as deleting, blocking or disconnecting links, and terminating transactions and services. A safe harbour from copyright liability to online platforms and service providers which take appropriate action after infringement is notified is similarly being contemplated in Hong Kong, where a consultation to amend the Copyright Ordinance and introduce a Code of Practice took place between November 2021 and February 2022. An amendment bill was published in May 2022 and then introduced into LegCo, Hong Kong's parliament, for consideration. It is expected to be passed before the end of 2022.

The APAC e-commerce and digital platform legal and regulatory landscape should be viewed against the backdrop of growing regulation in this area, including the proposed new EU legislation in the form of the Digital Services Act and the Digital Markets Act (for more, see our publications **The Digital Services Act – What is it and What Impact will it have?** and **Digital Services Regulation in the EU: An Evolving Landscape)**. From this perspective, retailers and consumer goods companies should consider the following issues and best practices:

- **Data privacy and security:** Given the contact details and financial information, as well as other personal data, inevitably provided by customers, compliance with the relevant data privacy legal framework is a key concern. Data audits should be conducted and data collected and stored minimised or limited to what is necessary. Data and privacy policies must be transparent and displayed clearly and conspicuously, including on websites. Cybersecurity needs to be considered, for example, in relation to the network infrastructure, including technological safeguards and controlling physical access.

- **Brand and intellectual property protection:** Infringement and counterfeiting are major threats to the value of brands and are prevalent in Asia. A proactive and consistent approach to the investigation of infringement should be adopted.

- **Deal-making:** Conducting thorough pre-transaction due diligence can reduce the chance that acquirers absorb a target company's problems, and must include investigating intellectual property ownership, business partners, supplier contracts, third-party service providers, employees, and distributors.

- **Liability and dispute resolution:** Online terms and conditions should be reviewed to deal appropriately with liability and dispute resolution, which are particularly important given the frequently cross-border nature of e-commerce.

4.1 Are there particular laws or regulations regulating online retailers and platform providers?

Jurisdiction	Consideration
Hong Kong	A number of laws and regulations in Hong Kong are particularly relevant to parties that conduct business activities online. The **Electronic Transactions Ordinance (Cap. 553) (ETO)** accords electronic records and signatures the same legal status as that of their paper-based counterparts. There is an exception for transactions involving government entities which require a digital signature supported by a recognised digital certificate. The **Banking Ordinance (Cap. 155) and Payment Systems and Stored Value Facilities Ordinance (Cap. 584)** require banks, deposit-taking companies, retail payment system operators (for example, Visa, Mastercard, UnionPay, JETCO and EPS) and stored-value facility (SVF) operators (such as Octopus, Alipay, WeChat Pay, Autotoll and PayPal) operating electronic payment services to be licensed or designated by the Hong Kong Monetary Authority (HKMA) subject to one or both ordinances. Initiatives introduced by the HKMA to promote electronic payments in Hong Kong include the Faster Payment System (enabling easy cross-bank / SVF operator transfers, via the use of a mobile phone number or an email address to act as the payee's account proxy) and the Common QR Code Standard for Retail Payments (facilitating a merchant in using a single QR code to accept payment via different payment service operators). It is noted that electronic records produced from electronic payments are subject to the ETO. In addition, as doing business online is merely another medium for conducting commercial activities, legislation regulating various aspects of commercial and trading activities is also applicable to commercial and trading activities conducted through electronic means. For example: The **Trade Descriptions Ordinance (Cap. 362)** prohibits unfair practices conducted by businesses, including misleading actions or omissions, aggressive commercial practices and "bait advertising". Bait advertising refers to a practice where a trader advertises products for supply at a specified price where there are no reasonable grounds for believing that the trader will be able to offer for supply those products at that price, or where the trader fails to offer those products for supply at that price. The **Control of Obscene and Indecent Articles Ordinance (Cap. 390)** has wide application, and in the context of e-commerce, regulates internet and mobile content. Indecent articles not suitable for those under the age of 18 may only be published subject to conditions, and obscene articles are prohibited from publication altogether. Indecent and obscene articles include those that are violent, depraved or repulsive. Further, businesses should ensure that their websites do not include content that infringes intellectual property, contains misrepresentations, or is defamatory. The **Personal Data (Privacy) Ordinance (Cap. 486) (PDPO)** regulates the collection and use of personal data, including online collection and processing, and direct marketing activities. In relation to cookies, the Privacy Commissioner for Personal Data (Privacy Commissioner) suggests that if third-party cookies are deployed, organisations explicitly state what kind of information such cookies collect and to whom the information will be transferred and for what purposes, as well as whether users have the option to choose whether to accept cookies and if so, the consequences for non-acceptance, such as affecting the proper functioning of the website. The **Sale of Goods Ordinance (Cap. 26)** protects consumers and governs contracts for the sale of goods, including providing for implied conditions for goods to be of merchantable quality, fit for purpose and corresponding to the description by the seller. The **Consumer Goods Safety Ordinance (Cap. 456)** provides that consumer goods must comply with approved and general safety standards or specifications.

Jurisdiction	Consideration
	The **Supply of Services (Implied Terms) Ordinance (Cap. 457)** protects consumers and governs contracts for the supply of services, including providing for implied terms such as requiring services to be carried out with reasonable care and skill and, where the contract is silent, within a reasonable time and for a reasonable charge. The **Misrepresentation Ordinance (Cap. 284)** provides for statutory remedies relating to fraudulent, negligent and innocent misrepresentation. The **Control of Exemption Clauses Ordinance (Cap. 71)** protects consumers and regulates exemption clauses in contracts. Clauses excluding or restricting liability for death or personal injury resulting from negligence are not effective. The validity of clauses in consumer contracts excluding or restricting liability for breach is subject to the test of reasonableness. The **Unconscionable Contracts Ordinance (Cap. 458)** applies to contracts for the sale or supply of goods or services. In considering whether a contract is unconscionable, the court looks at such factors as the relative bargaining positions of the consumer and the other party, and whether the consumer was able to understand the relevant documents. If a contract or part thereof is found to be unconscionable, the court may refuse to enforce the same, enforce the remainder without the unconscionable element, or limit the application of or revise any unconscionable part.
China	The PRC government is active in passing laws and regulations concerning e-commerce activities and making policies to promote the development of e-commerce business. The key laws, regulations and policies include the following: 1. Opinions of the General Office of the State Council on Accelerating the development of Electronic Commerce (2005) 2. Notice of the General Office of the State Council on Forwarding the Opinions of the Ministry of Commerce and Other Departments on Implementing Relevant Policies to Support the Cross-Border E-Commerce Retail Export (2013) 3. Official Reply of the State Council on Approving the Establishment of Cross-Border E-Commerce Comprehensive Pilot Zones in Tianjin and Other 11 Cities (2016) 4. Circular of the Ministry of Commerce, the Office of the Central Leading Group for Cyberspace Affairs and the National Development and Reform Commission on Issuing the 13th Five-year Development Plan for E-commerce (2016) 5. Circular of the Ministry of Commerce and Other Five Departments on Issuing the Special National Plan for the Development of E-commerce Logistics (2016-2020) 6. Service Norms for Third-party E-commerce Transaction Platforms issued by the Ministry of Commerce in 2011 7. Norms for the Accreditation of Exemplary E-commerce Enterprises issued by the Ministry of Commerce in 2010 8. Administrative Measures for Online Trading issued by the State Administration for Industry and Commerce in 2014 9. The PRC E-Commerce Law (draft) published by the PRC National Congress in 2016 for public comments 10. The PRC Cross-Border E-Commerce Service Rules (draft) published by the Ministry of Commerce in 2016 for public comments 11. The PRC Mobile E-Commerce Service Rules (draft) published by the Ministry of Commerce in 2016 for public comments

Jurisdiction	Consideration
Singapore	The Electronic Transactions Act 2010 (ETA) regulates contracts formed on the internet and accords e-contracts and e-signatures the same status as written contracts and signatures. In 2020, Enterprise Singapore and the Singapore Standards Council launched the first national standard, Technical Reference 76 (TR 76), on guidelines for e-commerce transactions. TR 76 can serve as a checklist for online retailers, and lays down best practices on providing responsive customer support. Online retailers also remain subject to the consumer protection legislation, including the Unfair Contract Terms Act 1977, the Sale of Goods Act 1979, the Misrepresentation Act 1967 and the Consumer Protection (Fair Trading) Act 2003. Sales or advertisements of certain products and services online are also subject to specific regulation: 1. Online gambling service providers are regulated under the Gambling Control Act 2022 2. Provision of online financial services and products is regulated under the Securities and Futures Act 2001 3. E-retailing of second-hand goods is regulated by the Secondhand Goods Dealers Act 2007
Japan	The Specified Commercial Transactions Act (Act No. 57 of 1976, as amended) (SCT) regulates certain categories of e-commerce. Such regulations include advertising and prohibiting attempts to fraudulently induce customers to enter into agreements. There are two laws regulating payments: 1. The Payment Services Act (Act No. 59 of 2009, as amended) (PSA), which regulates various electronic payment methods. Depending on the nature of the electronic funds, notification or registration is required. In addition, certain information (including the terms of use) must be made available to the public and a security deposit may be required (the minimum amount of such deposit being determined by the Act) to enable the reimbursement of the user in the event of bankruptcy of the operator 2. The Instalment Sales Act (Act No. 159 of 1961, as amended) (ISA) was not originally intended to regulate e-commerce, but given that credit cards are often used to pay for purchases, operators must be wary of falling foul of the requirements of this Act. If an operator allows payments in instalments, the operator will be subject to supervision by the relevant authority under the Act The Digital Platform Transparency Act (Act No. 38 of 2020, as amended) (DPTA) regulates "Specified Digital Platform Providers" (Article 4 of the DPTA). Certain online mall operators and app store operators such as Google are currently designated by METI as "Specified Digital Platform Providers" and are subject to certain disclosure and reporting regulations under the DPTA. In July 2022, the cabinet order of the DPTA was amended, and its scope has been extended to apply to (i) media-integrated digital advertisement platform providers whose annual turnover in Japan is ¥100 billion or more and (ii) advertisement intermediary digital platform providers whose annual turnover in Japan is ¥50 billion or more.

Jurisdiction	Consideration
Australia	In Australia, there are no particular laws which regulate online retail or platform providers. The same rules apply online as to "brick and mortar" retailers. Relevant legislation includes the following: 1. Privacy Act 1988 (Cth) applies to online entities, regulating how contact and personal information is kept and transferred 2. Spam Act 2003 (Cth) requires that online entities ensure that they have consent to receive messages from recipients, that messages identify who is sending the message and that there is an "unsubscribe" facility to allow recipients to opt out 3. Fair Trading Acts (differing State versions) which apply equally to online transactions The *Competition and Consumer Act 2010 (Cth)* / Australian Consumer Law regulates dealings between, and the conduct of, competitors and applies equally to online competitors. For more, see our Talking Tech publication **Google LLC Ordered to Pay a AUS$60m Penalty for Misleading Users about the Use and Collection of their Personal Location Data**, which was ordered by the Federal Court of Australia to be paid to the Australian Competition and Consumer Commission (ACCC), being the first public enforcement outcome arising out of the ACCC's Digital Platforms Inquiry.

4.2 Are there specific laws and regulations aimed at regulating internet service providers?

Jurisdiction	Consideration
Hong Kong	In Hong Kong, ISPs are regulated by the Telecommunications Ordinance (Cap. 106) and its subsidiary legislation. Under the Telecommunications Ordinance, no person may operate any public telecommunication networks or services unless a Public Non- Exclusive Telecommunications Service (PNETS) Licence from the Governor in Council or the Telecommunications Authority (TA) has first been obtained. A proposed amendment of the Copyright Ordinance (Cap. 528) (by way of the Copyright (Amendment) Bill 2022 published on 27 May 2022 (the 2022 Bill)) targeted at online service providers (OSPs) proposes to provide for a safe harbour to OSPs to limit their liability for damages or other pecuniary remedies for copyright infringement occurring on their platforms, provided the following conditions are met: (i) the OSP has taken reasonable steps to limit or stop the alleged infringement as soon as practicable after receiving notice of it, becoming aware that the infringement has occurred. or becoming aware of facts or circumstances that would inevitably lead to the conclusion that the infringement has occurred; (ii) the OSP has not received any financial benefit directly attributable to the infringement; (iii) the OSP accommodates and does not interfere with standard technical measures used by copyright owners to identify or protect their copyright works; and (iv) the OSP designates an agent to receive notices of alleged infringement and supplies the agent's name and contact details on its service. The 2022 Bill clarifies that OSPs are not required to monitor their services or actively seek facts that indicate infringing activity, except to the extent consistent with standard technical measures of copyright owners. Standard technical measures refer to those generally accepted by the industry that have been developed through an open and voluntary process by a broad consensus of copyright owners and service providers, are available to any person on reasonable and non-discriminatory terms, and do not impose substantial costs on service providers or burdens on their systems or networks. A bills committee was formed to consider the 2022 Bill, which is expected to be passed before the end of 2022. Also of relevance to internet service providers is the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO), which was amended with effect from 8 October 2021. Offences to criminalise doxing (online publication of identifying information about an individual such as his or her real name or home address without consent and with intent to harm, commonly arising out of a disagreement or for revenge or punishment or a form of cyberbullying or harassment) were created. The Privacy Commissioner was also empowered to serve notices for the cessation or restriction of disclosure of doxing content and carry out criminal investigation and enforcement. Internet service providers, as well as online social media and other platforms and websites, which are incorporated or registered in Hong Kong or have a place in business in Hong Kong, or which are overseas offering services in Hong Kong, should be aware that they may be requested to remove or block access to doxing content and will face fines and imprisonment if requests to do so are ignored. Such service providers and platforms should also review their terms and conditions, including on the disclosure of personal data of users and suspension of account, to facilitate compliance with cessation notices and the Privacy Commissioner's criminal investigation powers.)

Jurisdiction	Consideration
China	A number of laws and regulations regulate internet service providers in China, including the following: 1. The PRC Cybersecurity Law 2. Administrative Measures for Internet Information Services 3. Interim Measures for the Administration of Internet Advertising 4. Provisions on Protection of Personal Information of Telecommunication and Internet Users In general, a commercial internet information service provider is required to obtain approval for an operating permit from the competent telecommunications administration authority and a non-commercial internet information service provider must record its information with the competent telecommunications administration authority in China.
Singapore	The Infocomm Media Development Authority is the regulating authority. Its framework for the internet is embodied in the Broadcasting (Class Licence) Notification. Under the Internet Class Licence, Internet Content Providers, Internet Service Providers and Internet Access Service Providers are deemed automatically licensed and have to observe and comply with the Internet Class Licence Conditions and the Internet Code of Practice, the key focus of which is content regarded as offensive or harmful to Singapore's racial and religious harmony or national interest.
Japan	The primary legislation dealing with the regulation of internet service providers is the Telecommunications Business Act (Act No. 86 of 1984, as amended). Depending on the nature of the business in question, notification to, or registration with, the relevant authority may be required to provide a service. Applicable regulations may require compliance with technical standards, the implementation of management rules for telecommunications facilities, as well as notification/reporting obligations. In 2022, the Japanese government has so far requested 48 tech multinationals that continuously conduct business in Japan to register their global headquarters with the legal affairs bureau to comply with the Companies Act (Act No. 86 of 2005, as amended). In response to the request, certain global tech companies operating in Japan have registered their global headquarters in Japan. One of the reasons behind this request is for consumers' convenience when filing lawsuits domestically.
Australia	The Telecommunications Act 1997 (Cth) regulates carriers and service providers and sets out standard service provider rules in Schedule 2 of the Act. Compliance with the Act and the Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth) is required for internet service providers (ISPs), as well as any additional service provider rules which may be imposed by the Australian Communications and Media Authority. The Telecommunications (Interception and Access) Act 1979 (Cth) requires ISPs to retain specific datasets for at least two years, which must be encrypted and protected from unauthorised access or interference. Some data must be kept for the life of the account and for two years after the account is closed.

4.3 What penalties are involved if these laws and regulations are breached?

Jurisdiction	Consideration
Hong Kong	The penalties involved if offences are committed under these various pieces of legislation vary and include fines and/or imprisonment. The relevant authorities may also pursue or assist in pursuing civil compensation against those breaching certain provisions of these pieces of legislation.
China	In addition to criminal offences and civil liabilities that may be assumed by an online dealer or an internet service provider, administrative penalties may include: 1. warnings 2. confiscation of illegal gains 3. revocation of the Operating Permit 4. rectification actions and/or fines levied on internet service providers 5. suspension of operation or closure of the website concerned
Singapore	With respect to regulation of online retailers and platform providers: 1. Offences under the Electronic Transactions Act 2010 are punishable with a fine not exceeding S$20,000 or imprisonment for a term not exceeding six months, or both 2. Breaches of the Unfair Contract Terms Act 1977 or the Misrepresentation Act 1967 do not result in direct penalties being levied. However, such breaches may either preclude reliance on a contractual term that limits liability (if the Unfair Contract Terms Act is infringed) or provide the basis for a claim for damages (if the Misrepresentation Act is engaged) 3. Offences under the Consumer Protection (Fair Trading) Act 2003 are punishable with a fine or imprisonment or both, depending on the specific offence in question 4. Offences under the Gambling Control Act 2022 range from fines of various amounts to imprisonment or both, depending on the offence committed Breaches of the Personal Data Protection Act 2012 (in failing to secure individuals' personal data) may also attract sanctions and result in civil action by the affected individuals

Jurisdiction	Consideration
Japan	Failure to comply with the Specified Commercial Transactions Act (Act No. 57 of 1976, as amended) (SCT Act) may give rise to an order issued by the competent ministry (e.g., the Consumer Affairs Agency, the Ministry of Economy, Trade and Industry (METI) and the Financial Services Agency (FSA)) to take remedial measures or to order cessation of part or whole of the business for up to two years. In addition, failure to comply with the SCT Act (in cases of serious breaches of the Act such as (i) when a seller or a service provider makes misrepresentation in material aspects of a contract such as the purchase price to induce customers to enter into a sales contract in breach of Article 6 and (ii) when a seller or a service provider does not comply with the cessation order above in breach of Article 8) may give rise to a criminal penalty of imprisonment for a maximum term of three years and/or a fine of up to ¥3 million. If a representative or employee of a company commits such a failure, the company will be subject to a criminal fine of up to ¥300 million. Failure to comply with The Payment Services Act (Act No. 59 of 2009, as amended) (PSA Act) may give rise to an order issued by the FSA to take remedial measures, to cease part or whole of the business for up to six months or for the revocation of licence(s). In addition, failure to comply with the PSA Act (in cases of serious breaches of the Act such as when a service provider carries out cryptoasset exchange services without the licence required under the Act) may give rise to a criminal penalty of imprisonment for a maximum term of three years and/or a fine of ¥3 million. If a representative or employee of a company commits such a failure, the company will be subject to a criminal fine of up to ¥300 million. Failure to comply with the Instalment Sales Act (Act No. 159 of 1961, as amended) (ISA Act) may give rise to an order issued by the METI to take remedial measures or for the revocation of licence(s). Furthermore, failure to comply with the ISA Act may give rise to a criminal penalty of imprisonment for a maximum term of three years and/or a fine of up to ¥3 million. If a representative or employee of a company commits such a failure, the company will be subject to a criminal fine of up to ¥3 million. Failure to comply with the Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA) may give rise to an order issued by the Ministry of Internal Affairs and Communications (MIAC) to take remedial measures or for the revocation of licence(s). Further, failure to comply with the TBA (in cases of serious breaches of the Act such as when a service provider carries out "telecommunication business" without the licence required under Article 9) may give rise to a criminal penalty of imprisonment for a maximum term of three years and/or a fine of up to ¥2 million. The MIAC may also publicly disclose the names of those who have failed to comply with the TBA, together with any other information which the MIAC finds necessary. Failure to comply with the Digital Platform Transparency Act (Act No. 38 of 2020, as amended) (DPTA) (in case of a serious breach of the Act such as (i) a "Specified Digital Platform Provider" does not comply with disclosure obligations under Article 5 and (ii) despite the fact that the METI has issued a series of warnings and orders against the platform provider to have the provider comply with the obligations pursuant to Article 6, the platform provider still does not comply with the order without any valid reasons) may give rise to a criminal penalty of a fine of up to ¥1 million (Article 23 of the DPTA). If a representative or employee of a company commits such a failure, the company will also be subject to a fine, of up to ¥ 1 million (Article 25 of the DPTA).
Australia	ISPs who breach the *Telecommunications Act 1997* (Cth) and related Acts may be subject to pecuniary penalties of up to AU$10 million per offence. The Australian Communications and Media Authority can issue a direction to ensure that a service provider does not breach the Act and issue a formal warning if there is a breach. The Act also prescribes criminal offences, such as s 276, which relates to breaches in the use and disclosure of information. The s 276 offence is punishable by up to two years' imprisonment. Criminal sanctions are usually only used as a last resort where there are ongoing and wilful violations of the Act.

4.4 Are online or electronic contracts enforceable?

Jurisdiction	Consideration
Hong Kong	**Electronic Transactions Ordinance** Yes. According to section 17 of the Electronic Transactions Ordinance (Cap. 553) (ETO), a contract shall not be denied validity or enforceability on the sole ground that an electronic record was used for that purpose. However, there are exceptions for certain types of contracts under Schedule 1 of the Ordinance. The exceptions are unlikely to be relevant to e-commerce and include documents such as wills, trust documents, powers of attorney and some negotiable instruments. Documents including contracts may further be signed electronically or digitally (subject to the same exceptions). The ETO distinguishes electronic and digital signatures. It allows the use of electronic signatures for documents if neither party is, or is acting on behalf of, a government entity. For documents involving government entities, digital signatures must be used. In terms of electronic signatures, the method must be reliable and appropriate, and the other party must consent to the method. Acceptable methods include the application of an electronic image (jpeg file) of a signature, making a mark, or taking some action electronically to indicate consent. The sender typing his name at the bottom of an email has been recognised in Hong Kong and English case law to constitute an electronic signature. Digital signatures on the other hand must be supported by and generated within the validity of a certificate issued by a certification authority recognised under the ETO such as the Hong Kong Post Certification Authority. Digital signing may also be executed by way of iAM Smart, which makes use of biometrics in personal mobile devices to authenticate identities (with identities having originally been verified during an in-person registration process against Hong Kong Identity Cards). **Clickwrap and browse-wrap contracts** E-commerce might involve clickwrap and browse-wrap contracts. Clickwrap contracts are likely enforceable, whereas the position with browse-wrap contracts is less clear cut. A clickwrap contract is a contract which requires a user to actively indicate acceptance or agreement by, for example, clicking an “I Accept” or similar button or icon, ticking a box, or tracing a manuscript signature. A browse-wrap contract is a contract, the terms of which often appear as a hyperlink on the relevant website, which a user is taken to accept by the mere act of browsing and using the website. We are not aware of any case in Hong Kong specifically dealing with the enforceability of clickwrap or browse-wrap contracts. That said, it is a matter of considering traditional contractual principles of offer and acceptance, consideration and intention to create legal relations. Clickwrap contracts are defined by the user taking positive action to indicate agreement such as clicking or ticking a button or box. An English case held that a clickwrap contract where the relevant party clicks an “I Accept” button is enforceable. On the other hand, there is no definitive answer in relation to browse-wrap contracts by the English courts. Similarly, US case law has found browse-wrap contracts to be both enforceable and unenforceable with the cases very much turning on their individual facts. The facts go to the extent of actual awareness of the terms, or whether the user can be taken to have notice of the terms. Other legal issues surrounding online or electronic contracts are dealt with in this Talking Tech piece here including whether: products displayed on a website or app constitute a binding offer to supply upon acceptance; sellers on online auction platforms are bound to supply to the highest bidder; standard terms can be incorporated if communicated electronically; and electronic updates to the terms of use are binding.

Jurisdiction	Consideration
China	Yes. The PRC Civil Code allows the parties concerned to conclude a contract in written, verbal or any other form.
Singapore	Yes. Basic contractual principles continue to apply to contracts made on the internet and contracts concluded over the Internet are enforceable. This is reflected in Section 11 of the Electronic Transactions Act 2010 (ETA), which provides that a contract shall not be denied validity or enforceability solely on the ground that an electronic communication was used in the formation of the contract. Section 8 of the ETA also accords e-signatures the same status as written signatures.
Japan	Yes. Under Japanese law, online or electronic contracts are enforceable, as long as it is considered that one party presents their wish to enter into an agreement on certain terms and the other party accepts such terms. However, the Special Provisions to the Civil Code Concerning Electronic Consumer Contracts and Electronic Acceptance Notice Act (Act No. 95 of 2001, as amended) does impose certain regulations in relation to electronic contracts. For example, regarding the timing of acceptance, in the event that a customer wants to make a purchase and sets this out in an email, the contract will only be considered to have entered into existence after the email successfully reaches the shop operator. Another example of regulation relates to the prevention of "one-click fraud". In this regard, in order to effect entry into an online contract, the relevant operator must reconfirm the customer's wish to enter into a contract by, for instance, displaying a confirmation page prior to completing the sale and purchase. Otherwise, the customer may claim that the order was mistakenly made and, as a result, the contract may be held to be unenforceable.
Australia	Online and electronic contracts are deemed to be as valid as a paper contract. A transaction is not invalid purely because it took place electronically; however, this does not apply where a more specific provision of legislation requires otherwise. To ensure enforceability of a contract it is recommended that there be: unambiguous notice to the customer that the transaction is governed by terms of contract law; an option for the customer to review the terms prior to agreement; and a clear statement as to what constitutes agreement.

4.5 What should I be aware of when advertising online?

Jurisdiction	Consideration
Hong Kong	**Metatags and search engine optimisation** Many companies adopt "search engine optimisation" (SEO) strategies as marketing tactics to attract online traffic. By doing so, website owners may rely on metatags to improve their rankings in search engines' results pages. However, this also raises the question whether a website owner would be infringing upon the rights of others if the metatags (the invisible data on their website) they have chosen include registered trademarks belonging to others. In the Hong Kong case of *China National Gold Group Corp. v China (HK) Gold Group Shares Ltd*, HCA 699/2013 (unrep., 17 September 2013), the court indicated that the defendant's act of infringement and passing off was aggravated by material contained in the defendant's website that included "metatags" which had the effect of giving prominence to the defendant's material in a search engine on the internet, and which of itself constituted trademark infringement. There has also been a court case on this metatag trademark infringement issue in Japan. **Spam** Spam or digital promotional mail that is unsolicited may be sent provided that the requirements under the Unsolicited Electronic Messages Ordinance (Cap. 593) (UEMO) and the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) are met. The UEMO regulates unsolicited electronic messages for advertisement, promotion or offering to supply goods, services or business or investment opportunities by email, instant messaging or other media. The UEMO requires the relevant electronic message to: (i) contain accurate information about the sender's identity and contact details; (ii) contain an unsubscribe facility; and (iii) not use a misleading subject heading. In addition, the sending of electronic messages using address-harvesting software or a harvested address list without addressee consent is a criminal offence under the UEMO. The PDPO regulates the collection and use of personal data including for direct marketing. "Spam" will involve personal data and trigger the application of the PDPO if it identifies the intended recipient. Consent of the recipient must be sought. Other requirements to be aware of in relation to direct marketing are that written consent is required for data transfers (even to subsidiaries or associated companies). There must be notification of certain rights such as of opt-out and to request access to and correction of data collected. Further, personal data handling policies must be published. Contravention of some of these requirements carry criminal sanctions. **Trade Descriptions Ordinance** Apart from the use of metatags and "spam" to promote products and services online, there are also general offences under Hong Kong law (for example, under the Trade Descriptions Ordinance (Cap. 362) (TDO)) of which online advertisers should be aware. For example, sections 7 and 7A of the TDO prohibit false trade descriptions in relation to goods and services. Furthermore, under section 13E of the TDO, a trader who engages in a commercial practice that is a misleading omission commits an offence. Under section 13G of the TDO, any person who commits bait advertising also commits an offence. Both offences constitute "*unfair trade practices*" as outlined under the TDO. An innocent publication defence is available to those involved in the business of publication of advertisements.

Jurisdiction	Consideration
	Industry-specific advertising restrictions Depending on the type of goods or services promoted, other industry-specific advertising restrictions may apply. For example, advertisements of financial services and products may need to meet certain requirements under the Securities and Futures Ordinance (Cap. 571) (SFO) and codes and guidelines published by the Securities and Futures Commission (SFC). For example, the **advertising guidelines applicable to collective investment schemes** and the **guidelines on online platforms and advisory services:** the latter requires up-to-date product offering documents; information as to the scope and limitations of services; and disclosure of commission, and brokerage and other fees. Other advertising restrictions in relation to food, drugs and the medical sector apply by virtue of the Public Health and Municipal Services Ordinance (Cap. 132); Food and Drugs (Composition and Labelling) Regulations (Cap. 132W) and Undesirable Medical Advertisement Ordinance (Cap. 231). **Other developments** A significant proportion of a brand owner's marketing budget is now likely to be allocated to advertising through social media platforms. Increasingly, such advertising takes the form of the use of "influencers". Influencers are individuals who have developed a large (and loyal) following of consumers on social media platforms. When the influencer recommends or endorses a product by way of a favourable social media post, the brand owner seeks to benefit by the influence of followers' purchasing decisions. In many respects, engaging influencers is similar to engaging other types of well-known individuals to provide endorsements such as actors or musicians. The fact that influencers engage almost exclusively through social media does, however, create some additional challenges, as well as requiring a different approach to more traditional endorsement. For the key points brand owners should bear in mind when engaging influencers to participate in marketing campaigns, including the right influencers; the right audience; the right content and channels for sharing content; and managing risk, see our Talking Tech publication Influencer marketing – key considerations for brand owners.
China	The PRC Interim Measures for the Administration of Internet Advertising issued by the State Administration for Industry and Commerce in 2016 are the measures that particularly regulate online advertising activities in China. This rule applies to commercial advertisements that promote commodities or services, directly or indirectly, via online media such as websites, webpages and online application programs, in the form of texts, pictures, audios, videos or in other formats. No advertisements for any medical treatments, medicines, foods for special medical purpose (FSMP), medical apparatus, pesticides, veterinary medicines, dietary supplements or other special commodities or services may be published unless they have been reviewed and approved by an advertising examination authority. The following online advertising activities are prohibited: 1. providing or using any application programs or hardware to intercept, filter, cover, fast forward or otherwise restrict any authorised advertisement of other persons 2. using network pathways, network equipment or applications to disrupt the normal data transmission of advertisements, alter or block authorised advertisements of other persons, or have advertisements load without authorisation 3. using false statistical data to induce incorrect quotations and/or damage the interests of other persons

Jurisdiction	Consideration
Singapore	All advertising and marketing activities, including online advertising, are guided by the Singapore Code of Advertising Practice (SCAP). While the SCAP does not have the force of law, it provides general and certain industry-specific guidelines that all advertisements must comply with. As in Hong Kong and Japan, many companies in Singapore adopt "search engine optimisation" (SOE) strategies as marketing tactics to attract online traffic. By doing so, website owners may rely on metatags to improve their rankings in search engines' results pages. However, this also raises the question of whether a website owner would be infringing others' rights if the metatags (the invisible data on their website) they have chosen include the registered trademarks of others. (The question has been answered in the affirmative in cases in Hong Kong and Japan.) The Spam Control Act 2007 imposes specific requirements on bulk commercial messages sent electronically. For instance, the e-mails must labelled with <ADV> and must contain an "opt-out" function.
Japan	The legislation of primary relevance is the Act against Unjustifiable Premiums and Misleading Representations (Act No. 134 of 1962, as amended). This Act applies to a broad range of advertisements. The object of the Act is to ensure that advertisements are clear about the applicable terms and conditions, as well as the nature of the relevant goods or services. To prevent misleading information, even matters such as the font and formatting of hyperlinks are regulated. In addition, as referred to above, the SCT Act regulates advertisements, including false trade descriptions, as well as restrictions on email advertisements addressed to recipients who have not provided their consent to receive them. Stakeholders seeking to take advantage of cutting-edge advertising methods (such as "search engine optimisation" (SOE) or targeted behavioural advertising) should be wary of falling foul of legislation protecting intellectual property (such as trademark rights) and personal data. This is particularly so in light of a District Court ruling that held, on the specific facts of that case, that metatags (the invisible data on the relevant party's website) infringed another party's trademarks. There has also been case law on this issue in Hong Kong.
Australia	The Spam Act 2003 (Cth) regulates spam mail, requiring advertisers to obtain consent before initiating commercial electronic messaging, identify the sender/business and ensure customers have the ability to unsubscribe from future messages. The Privacy Act 1988 (Cth) sets out requirements for data handling practices to ensure personal data is dealt with in an open and transparent manner. This plays a role in online advertising as many interactive forms of advertisements collect and use data to measure and profile advertising. With regards to bodies that regulate the industry, the Australian Competition and Consumer Commission regulates digital advertising through the Australian Consumer Law, setting out basic standards including regulation of misleading and deceptive conduct, and false and misleading claims. The Australian Communications and Media Authority handles the day-to-day regulation of electronic communications, including the handling of complaints. Breaches of the regulations and laws will lead to investigation by these authorities, and more serious breaches can lead to infringement notices or court-imposed fines.

PERSONAL DATA PROTECTION AND SECURITY

5. PERSONAL DATA PROTECTION AND SECURITY

Data is at the core of successful digital products. What is done with that data is not only pivotal to enhancing customer satisfaction, but also to winning consumers' trust and remaining competitive.

With connectivity comes the creation of data associated with a given object. With the creation of data comes the likelihood that it will be collected, aggregated, used or misused, for good or ill. Creation of data brings the recognition that the data itself is valuable (in some cases more valuable than the connected object itself) as well as the desire to leverage the data for profit and commercial purposes.

As a hypothetical example, think of a "connected" pen. What personal information might be derived from its use? You could track someone's location as the pen sits in a wallet or purse, collect and transmit geolocation information, information about the stores and restaurants visited by the user and perhaps even the individual shop counters within the store that the user visits, such as the aisle in which pregnancy tests are available.

The "content" created by the pen, in other words the data it records, is tracked. This might include the people or companies to whom cheques are written and the amounts, private messages passed between friends and family, or even trade secrets associated with a business proposal. To take another example, a mobile phone could record audio and video and transmit back to the manufacturer for further use and analysis.

When IoT is fully implemented, the range and volume of potentially personal or private information that will be made available to third parties will be enormous. This poses risks for consumers as well as the companies seeking to collect and use that information for whatever purpose.

Local legislation and legislation such as the GDPR with extraterritorial effect

Currently, most legislation is aimed at regulating the protection of personal information. When dealing with overseas companies or suppliers, care must be taken to comply with local legislation.

Care must also be taken to comply with data protection legislation with extraterritorial effect. The GDPR came into effect on 25 May 2018 and applies to non-EU companies where goods or services are provided into the EU or where personal data is obtained in the EU and transferred outside. Thus, even companies with no presence in the EU should assess, for example, whether any online activity results in the processing of personal data for the purposes of the GDPR, such as websites and apps directly offering goods or services to individuals in the EU, or cookies or other tracking activities monitoring the behaviour of individuals within the EU. Further, the GDPR now regulates data processors in some key respects, including in relation to information security and record-keeping. (Data processors are third-party service providers processing data on behalf of data controllers. Previously, only data controllers deciding on the purpose and means of processing were subject to EU data protection law.)

"In today's information economy, data is the new oil. A business' ability to transfer and use customer data and other information is both integral to the day-to-day running of a company and key to profitability and success. With more stringent data privacy laws, in particular the EU General Data Protection Regulation (GDPR) and key jurisdictions in APAC following suit such as the introduction of the PRC Personal Information Protection Law (PIPL), it is important that businesses are fully informed and compliant. Companies managing increasingly complex and fragmented data protection compliance programmes will be paying attention to developments in international data transfer, sensitive data processing, targeted advertising, data monetisation, self-sovereign identities, IoT and ransomware attack response."

Case Study: First Court Decision in which GDPR applied to non-EU company

The first court decision in France holding that the GDPR applied to a non-EU (Canadian) company was issued on 2 August 2019. On the facts, the Canadian company claimed that hundreds of audio-visual works in which it owned the IP were being made available for illegal download. The Canadian company instructed a German entity to identify the associated IP addresses and then asked a Paris court to compel the telecommunications service provider to supply the contact details of the holders of the IP addresses. The Paris court held that the collection of IP addresses was data processing, a large portion of which took place in France, and corresponded to the monitoring of behaviour of individuals in the EU. The Canadian company was held to be a data controller and should have ensured the security of the personal data. The Paris court refused the request for the contact details of the persons holding the IP addresses.

See also **Controversial Decision: Are Cloud Services Provided by European Subsidiaries of US Companies Illegal?**

GDPR requirements

In addition, the GDPR now provides for tighter requirements to obtain valid consent from individuals to process data and an expanded list of mandatory information to be provided to individuals to inform them of the usage of such data. For more, see our Talking Tech publication **Who Do You Share My Data With? AG Pitruzzella Weighs In on the Debate**. IT systems must be technically capable of supporting GDPR compliance. The right to be forgotten and right of data portability impact IT systems' capability and design.

It is mandatory for data controllers to notify data breaches to the relevant supervisory authority within 72 hours of becoming aware of the same, as well as to notify relevant data subjects of high-risk breaches without undue delay. A high risk is defined by reference to risk to the rights and freedoms of natural persons such as risk of discrimination, identify theft or fraud, financial loss or damage to reputation. Disclosure of data revealing racial or ethnic origin, political opinion, sexual habits, religion or genetic data is likely to damage individuals. A data controller is taken to be aware when it has a reasonable degree of certainty that a security incident compromising personal data has occurred. For example, if a USB key with unencrypted personal data is lost, a data controller is taken to be aware when it learns the key is lost even if it has not assessed whether unauthorised people have gained access to it.

GDPR penalties for breaches

Failure to comply with the GDPR exposes a company to sizeable penalties for serious breaches – up to €20 million or 4% of global turnover, whichever is higher.

Case Studies: British Airways and Marriott

On 8 July 2019, the UK privacy regulator, the Information Commissioner's Office (ICO), issued a notice of intention to impose an unprecedented fine of £183.4 million against British Airways (BA), being 1.5% of BA's global turnover for 2017. This arose from a cyber incident in June 2018 whereby customers attempting to access the BA website were rerouted to a fraudulent website following which personal details were stolen. The personal data of 500,000 BA customers was compromised due to BA's poor security arrangements. The ICO made clear that adequate protection of personal data is key and businesses are expected to invest in data and cyber compliance in proportion to their turnover. The ICO further confirmed that BA did co-operate with investigations and has since made improvements to its security arrangements. Thus, how businesses handle incidents after discovery will not entirely mitigate liability.

The ICO subsequently issued a second notice of intention to impose another radical fine; in this case, in the sum of £99.2 million against Marriott International, Inc (Marriott). This arose from a cyber incident in November 2018 in which 339 million guest records, including credit card details, were stolen. The ICO flagged that the data vulnerability could be traced back to the compromised systems of Starwood Hotels and Resorts (Starwood) which was acquired by Marriott in 2016, and insufficient due diligence had been undertaken when Marriott acquired Starwood.

Data litigation

The risks to businesses of civil claims arising out of data breaches have been underplayed. Data litigation is on the rise and the exposures are potentially significant. Not only were BA and Marriott fined by the ICO for GDPR breaches as discussed in the case studies above, but they also face multibillion-pound civil claims. Google also faced potential multibillion liability in the *Lloyd v Google LLC* representative action. The BA group action is opt-in and requires claimants to sign up. According to the case management decision *Weaver and Others v British Airways Plc* [2021] EWHC 217 (QB), as of February 2021, some 23,000 claimants had signed, representing almost 5% of the 500,000 BA customers affected. The lead law firm, PGMBM, reached a settlement with BA in July 2021. The terms of settlement are confidential, but damages of £2,000 per claimant had been indicated in the PGMBM invitation to sign (whilst another law firm, Your Lawyers, indicated damages of £6,000 per claimant). Claims brought by other law firms have yet to settle.

On the other hand, the potential representative action faced by Google (involving some 4 million smartphone users whose Internet activity had been tracked) provided for an opt-out mechanism and the damages faced were on a different scale even if the damages per claimant were lower, at £750. The decision of the Supreme Court, handed down in November 2021, determined that loss of control of personal data alone is insufficient and evidence of material damage or distress is required for compensation for breach of statutory privacy rights. Further, the members of the representative class must have the same interest in the claim (including damages being calculable on a common basis) and must be identifiable for a representative action to proceed. Such elements were not met and the door to the representative action has thus been closed. For more, see our briefing **Lloyd v Google: How the Supreme**

Court judgment closed the door on Lloyd's £3.3 billion data claim. Marriott faces a representative action in England, which was commenced in August 2020 and financed by litigation funding.

In broad terms, data claims can be split into two categories: (i) misuse of data held and (ii) data breach and malicious action by a third party such as a cyber-attack. The BA and Marriott cases were in category (ii), and the Google case in category (i). Data claims might involve allegations of breach of confidence or other tortious duty of care, breach of contract, or GDPR or other statutory breaches concerning requirements for adequate systems. Issues such as having a communications protocol in place to ensure legal professional privilege and appropriate notification to relevant regulatory authorities need to be considered. Key defences and arguments to challenge these claims might relate to, for example, the relevant information not being confidential in the first place and already being in the public domain; lack of causation and adequate mitigation (a third party caused the cyber-attack and mitigation measures were taken such as immediate notification to data subjects); and reducing the quantum of damages. See **our briefing on the growing risk of group litigation and class actions** including the large amounts of damages being claimed by data subjects, which discusses a rise in claims for data breach including shareholder and customer claims and data misuse class actions, as well as **our briefing exploring the key defences and arguments available** in light of the emerging case law to challenge such claims. See also **our Talking Tech article regarding a European Court of Justice decision strengthening the position of consumer protection associations**, which may now bring representative actions against data protection violations; this will have a particular impact on companies operating in the B2C sector, as their compliance with the GDPR is closely monitored by such associations.

Takeaways for APAC companies

Asia Pacific-based companies need to be aware of the potential exposure to regulatory investigations, sanctions, claims from individuals and class actions, as well as criminal liability. They should consider not only financial, but also reputational risks. Lessons to be learnt from the BA and Marriott cases include the need for due diligence of cyber risks in the form of detailed legal and forensic systems testing, and protection through deal documentation; sophisticated audit and testing for compliance with the GDPR (to match that in place for financial audit) to be designed with technical and legal collaboration; and, in line with the link between levels of turnover and investment, large and sophisticated businesses should ensure ongoing investment in similarly sophisticated compliance programmes that will deal with constantly evolving risks.

5.1 What are the main personal data protection laws in your jurisdiction?

Jurisdiction	
Hong Kong	The main legislation regulating personal data privacy and protection is the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). Everyone who is responsible for controlling data (Data User) should follow the six Data Protection Principles (DPPs) which represent the core of the PDPO covering the life cycle of a piece of personal data of a living individual known as the data subject. Personal data is defined as data from which it is practicable to ascertain the identity of the data subject, and which is in a form in which access and processing is practicable. Although a contravention of the DPPs does not constitute an offence in and of itself, the Privacy Commissioner for Personal Data (the Privacy Commissioner) may serve an enforcement notice on a data user for contravention of the DPPs to direct the data user to remedy the contravention. A data user who contravenes an enforcement notice commits an offence and is liable on first conviction for a fine of up to HK$50,000 and imprisonment for a maximum term of two years. The PDPO provides for a number of exemptions; for example, there are general exemptions for personal data held for domestic or recreational purposes. Data subjects who suffer loss or damage as a result of a breach involving data related to them may also institute civil claims against the data users concerned. Section 66 of the PDPO provides that an individual who suffers damage by reason of a contravention of a requirement under the PDPO may be entitled to compensation. Section 33 of the PDPO, prohibiting transfer of personal data to places outside Hong Kong unless specified exemptions or conditions are met, is not yet in force and no timetable has been fixed for its implementation. Nevertheless, due to increasing digitalisation and globalisation, in May 2022, the Privacy Commissioner published model contractual clauses for cross-border transfers of personal data by way of guidance (supplementing earlier guidance published in December 2014). The Privacy Commissioner advises the incorporation of such clauses as part of taking reasonable precautions and exercising due diligence to ensure data is not used in the transferee's jurisdiction in a manner contrary to the PDPO if use had taken place in Hong Kong (which is a condition under section 33). Despite section 33 not being in force, compliance should seriously be considered to avoid any potential liability and reputational damage with data users / controllers remaining responsible for data breaches (as opposed to data processors). There are other industry-specific obligations that may have to be complied with. For example, in the financial industry: • The Hong Kong Monetary Authority (HKMA) Customer Data Protection Circular of October 2014; Use of Personal Data in Fintech Development Circular of May 2019; Consumer Protection (including Data Privacy and Protection) in respect of Use of Big Data Analytics and Artificial Intelligence Guiding Principles of November 2019; Sharing of Customer Data for Direct Marketing by Third Parties Guidance of November 2021; Sound Practices for Customer Data Protection Circular of April 2022 following a thematic examination; and The Sharing and Use of Consumer Credit Data through Credit Reference Agencies Supervisory Policy Manual module. • The Securities and Futures Commission's (SFC) guidance centres on cybersecurity, which is covered in section 6, albeit data privacy and protection are discussed in the Use of External Electronic Data Storage Circular of October 2019, Internet Trading Cybersecurity Circular of September 2020 and Operational Resilience and Remote Working Circular of October 2021. • The Insurance Authority (IA) Guideline on the Use of Internet for Insurance Activities (GL 8) and Guideline on Cybersecurity (GL 20). • The Privacy Commissioner has also issued industry-specific guidance, for the banking industry in October 2014 and for the insurance industry in November 2012.

Jurisdiction	
China	**PIPL** On 1 November 2021, the PRC Personal Information Protection Law (PIPL) took effect. The PIPL is a landmark in the regulation of personal information in the PRC and puts in place a comprehensive data privacy regime. It forms a core component of the PRC's legal framework governing data, alongside the Data Security Law and the Cybersecurity Law. While certain features of the PIPL reflect a focus on national security and digital sovereignty that is consistent with the policy priorities of the PRC government, the emphasis on protection of the rights of individuals against abuses by businesses that process their data aligns with the growing international consensus around robust and comprehensive laws that treat the privacy of individuals as a key concern in the regulation of technology. In terms of the PIPL's scope of application, it applies to the processing of personal information that takes place in the PRC; or which is conducted outside of the PRC, to the extent such activities are carried out to process the personal information of persons within the PRC, and such processing is for the purpose of providing products or services to persons in the PRC or to analyse or assess the behaviours of persons in the PRC. Overseas companies subject to the PIPL will be required to establish a dedicated entity or appoint a representative within the PRC that will be responsible for matters related to their personal information processing. Foreign processors endangering China's national security, the public interest or private personal information rights, may be put on a restricted or prohibited list. Bases on which personal information can be transferred outside the PRC pursuant to the PIPL include: (i) passing a security assessment organised by the relevant cybersecurity administration body; (ii) having obtained personal information protection verification by a specialised institution recognised by the cyberspace administration; or (iii) having executed a standard form data contract formulated by the cyberspace administration with the offshore data recipient, known as China Standard Contractual Clauses (China SCCs). At the time of writing, a consultation draft of China SCCs and relevant regulatory rules guiding the use of China SCCs have been issued. China SCCs are expected to provide a convenient basis for export similar to standard contractual clauses under the European Union's GDPR (albeit relevant export activities must satisfy the eligibility conditions for using China SCCs). The export of personal information triggers certain requirements irrespective of the amount of personal information being exported, such as ensuring the offshore data recipient processes and protects the personal information exported to the same standard as that provided for in the PIPL; obtaining data subject consent for export; and self-assessment of the potential impact on data protection and data subject rights. If the amount of personal information being exported reaches a certain threshold or the relevant processor is a critical information infrastructure operator (CIIO), China SCCs will not be applicable and the relevant party needs to pass a security assessment as referred to in basis (i) above for the export of personal information. Further, the PIPL prohibits the provision of personal information stored in China to foreign judicial or enforcement authorities without proper consent from competent PRC authorities. Whilst many key concepts and rules are similar to those seen internationally in privacy regulations, especially the GDPR, there are significant differences in the detail. Multinational companies will need to be mindful of these differences when considering their compliance processes and controls. For more, see our **client briefing on the PIPL**. See also our **alerter on China SCCs** and **alerter on security assessment**.

Jurisdiction	
	DSL The Data Security Law (DSL) took effect on 1 September 2021. Together with the PIPL, the DSL is a cornerstone of China's legal framework on data. The DSL is also an important pillar for the country's national security regime. It is a key supplement to the Cybersecurity Law issued in 2016, which imposes cybersecurity requirements on network operators. The DSL is primary legislation that lays down the overarching legal framework and high-level principles on data processing including collection, storage, use, transmission and disclosure of data (including important data). Detailed guidance is expected to be provided in subsidiary and local regulations, industry guidance and/or judicial interpretations by the PRC Supreme People's Court. The application of the DSL is broad, affecting companies and individuals processing data in China, as well as data originating from or relating to China, if its processing impairs national security, the public interest or private rights in China. Hence, multinational companies outside China which transmit data collected in China to their overseas offices need to pay particular attention to the potential extraterritorial effect of the DSL (subject to the practical ability of Chinese authorities and courts to exercise jurisdiction over overseas companies). The DSL ranks data with regard to the significance of such data to national security, the public interest and potential harm arising from any breach. National core data and important data are subject to higher levels of protection and use supervision. Companies must determine whether they are processing important data, and, if so, certain requirements under the DSL will be applicable, in particular: • appointing a designated person to be responsible for the security of important data; • conducting a periodic risk assessment on the processing activities of important data, with the assessment report to be submitted to PRC regulators; and • compliance with rules on storage within the PRC and security assessment for the export of important data. This extends storage and export requirements for important data, which had already applied to CIIO under the Cybersecurity Law. The Security Assessment Measures for Data Export published by the CAC came into effect on 1 September 2022. As for what constitutes important data, in line with the grading system under the Cybersecurity Law, the DSL states that, at the national level, a data classification and grading system will be established. The central government will co-ordinate with different authorities to formulate a catalogue of important data with input from local governments and industry regulators. Other than the regulation of export of important data, a further restriction to be aware of regarding the export of data is that the DSL prohibits the provision by persons in China of data stored in China to any foreign judicial or enforcement authority without approval from a competent Chinese authority. The DSL does not provide specific rules on the approval procedure, and relevant implementation rules are expected to be announced. It is also noted that the PRC Export Control Law (governing export licensing or export bans of technical information and data related to controlled items) and the PRC Administrative Regulations on Technology Import and Export (TIER) (governing exports including by way of assignment of technical secrets) may also come into play and apply to the export of data. The potential interplay of various laws and regulations highlights the importance for companies to appoint professionally qualified individuals who are conversant with the law and local practice to oversee data transfer. For more, see our **client briefing on the DSL** and **global IP update publication on the DSL**.

Jurisdiction	
Singapore	The key personal data legislation in Singapore is the Personal Data Protection Act 2012 (PDPA) which provides a baseline standard of protection for personal data. The PDPA comprises various rules governing the collection, use, disclosure and care of personal data. The 2020 amendments to the PDPA strengthen organisational accountability and consumer protection. The PDPA recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. It protects personal data stored in both electronic and non-electronic forms. The PDPA complements sector-specific legislative and regulatory frameworks, such as the banking secrecy obligations contained in the Banking Act.
Japan	The Protection of Personal Information Act (APPI) was enacted in May 2003 and major amendments were implemented in May 2017, and another major amendment was implemented in April 2022. The purpose of the amendments in May 2017 was to increase the level of protection of personal information to the same level as in the European Union by, among other things, establishing the Personal Information Protection Commission (kojin joho hogo iinkai) (PIPC) as a central regulatory body to supervise the protection of personal information, introducing a definition of "sensitive data" and "anonymisation", and imposing additional restrictions on the transfer of data overseas. The amendments implemented in April 2022 introduced stricter restrictions on the transfer of personal data including the cross-border transfer of personal data and the concept of "pseudonymisation", which contributes to the use of personal data in the process of utilising AI. The APPI applies to the private sector. The PIPC was established on 1 January 2015 as the sole regulatory body under the APPI and is responsible for regulating and supervising all private industries. The PIPC has since issued guidelines (PIPC Guidelines) on the protection of personal information amended guidelines in accordance with the amendments implemented in April 2022 were issued in October 2021) in order to provide more detailed guidance on how to comply with the APPI. All private industries are subject to the PIPC Guidelines. In addition, where the PIPC delegates part of its power to certain governmental agencies due to their expertise, such agencies have issued guidelines which apply specifically to their sector. For example, the Ministry of Internal Affairs and Communications (MIAC) has issued guidelines on the protection of personal information applicable to business operators regulated under the Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA). The TBA was amended in June 2022 (to be implemented by no later than June 2023) and new amendments will require registrable/notifiable telecommunication business operators and certain other telecommunication business operators which do not have to be registered with or notified to the MIAC (so-called "Item 3 Operators", examples of which include online shopping malls and online storage services), to notify, announce, obtain consent from users or implement "opt-out" measures when transmitting the details of user information to third parties

Jurisdiction	
Australia	The Australian Privacy Principles (APPs) regulate the manner in which personal information is managed, collected, dealt with and maintained by government agencies and private sector organisations. Personal information is defined as information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not. The APPs are found in Schedule 1 of the Privacy Act 1988 (Cth) (Privacy Act). The APPs apply to Australian government agencies and private sector organisations with an annual turnover of more than AU$3million. The Privacy Act does not distinguish between data controllers and data processors. All entities to which the Privacy Act applies are subject to the same obligations. In addition, due to its extraterritorial effect, the Privacy Act applies to the acts and practices of foreign organisations with an 'Australian link'. There are 13 Australian Privacy Principles. They govern standards, rights and obligations around: • the collection, use and disclosure of personal information; • an organisation or agency's governance and accountability; • the integrity and correction of personal information; and • the rights of individuals to access their personal information. The APPs are principles-based law. This gives an organisation or agency flexibility to tailor their personal information handling practices to their business models and the diverse needs of individuals. They are also technology neutral, which allows them to adapt to changing technologies. There are other federal laws relevant to data protection, including: 1. **Do Not Call Register Act 2006 (Cth)**: This Act establishes restrictions regarding unsolicited telemarketing calls; 2. **Spam Act 2003 (Cth)**: This Act establishes restrictions regarding the sending of commercial electronic messages; and 3. **Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)**: This Act establishes obligations regarding compliance with the APPs in respect of information obtained under this Act. Additionally, there are sector-specific laws that impact data protection such as the *Telecommunications Act 1997 (Cth) and Telecommunications (Interception and Access) Act 1979* (Cth) for the telecommunications sector, and the *My Health Records Act 2012 (Cth) and the Healthcare Identifiers Act 2010* (Cth) for the health sector. There are also a range of state and territory laws which regulate personal data protection (such as the *Privacy and Personal Information Protection Act 1988* (NSW)) which apply to personal information held by, inter alios, government agencies.

5.2 Are there any mandatory technical and organisational security measures in place to protect personal data?

Jurisdiction	
Hong Kong	While there are no statutory requirements to put in place technical and organisational security measures to protect personal data, data users should be aware of the following: 1. Data Protection Principle 4 of the PDPO requires that data users must take all practicable steps to ensure that personal data is protected against unauthorised or accidental access, processing, erasure, loss or use. Businesses must ensure that measures providing an appropriate level of cybersecurity are applied where technology is engaged, such as internet transactions that involve the transmission of personal data. 2. The guidance dealing with Privacy Management Programmes, published by the Privacy Commissioner in February 2014 and updated in March 2019, makes clear that significant organisational measures are the expected standard for compliance. The Privacy Commissioner also issued a Guidance Note on Data Security Measures for Information and Communications Technology in August 2022 covering organisational measures, as well as data governance and technical and operational security measures.
China	The PRC Civil Code, which took effect on 1 January 2021, contains a chapter on personal information protection and privacy rights. The Civil Code requires the implementation of technical measures to protect personal information that has been collected and stored from being tampered with, leaked, or lost. Pursuant to the Data Security Law (DSL), if important data is being processed, data processors are required to enhance risk monitoring, identify system loopholes, and report and take immediate measures to cope with data incidents. Article 51 of the Personal Information Protection Law (PIPL) also requires the implementation of proper organisational and technical measures to protect personal information that has been collected and stored from being tampered with, leaked, or lost. Such measures include: (i) putting in place internal management structures and formulating operating rules; (ii) implementing tiered personal information management, and adopting corresponding technical security measures such as encryption, as well as anonymisation as appropriate; (iii) determining and periodically reviewing levels of access for employees handling personal information processing; (iv) conducting regular employee training; and (v) developing contingency plans for personal information security incidents. In addition, network operators are required by the PRC Cybersecurity Law to take technical and other necessary measures to safeguard network operations from interference, destruction or unauthorised access, and to prevent network data from being tampered with, leaked, or stolen. Network operators should take care to maintain the integrity, confidentiality and accessibility of network data.
Singapore	Under the PDPA, organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks and the loss of any storage medium or device on which personal data is stored. For example, these may include requiring employees to adhere to confidentiality clauses in their employment contracts or adopting technological safeguards to secure the personal data and the computer networks which contain them. Further, where an organisation employs a data intermediary to process personal data on the organisation's behalf and for the organisation's purposes, the organisation retains the same obligations under the PDPA as if the personal data were processed by the organisation itself.

Jurisdiction	
Japan	Under the APPI, necessary and appropriate measures to protect personal data must be taken. The PIPC has included in the PIPC Guidelines details of such measures. The PIPC Guidelines are not considered "hard law" but, in practice, act as "soft law" that should be followed by enterprises. The new amendments to the Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA) (to be implemented by no later than June 2023) will introduce obligations on certain large telecommunication business operators (to be designated by law) to implement and file with the MIAC information management protocols (with respect to security management, monitoring of subcontractors, information policy, and self-assessment of the treatment of user information through the so-called PDCA (Plan Do Check Action) cycle) and the appointment of responsible person(s) to supervise and prevent leakage of user data within three months from the date of such appointment. Please note that "users" under the TBA are not limited to individuals and include corporate customers.
Australia	There are no particular security standards that are required by law; however, APP 11 imposes a general obligation to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference or loss. It also requires protection from unauthorised access, modification and disclosure. Additionally, where an entity no longer needs personal information for any purpose for which the information may be used or disclosed under the APPs, the entity must take reasonable steps to destroy the information or ensure that it is anonymised. This requirement is subject to limited exceptions.

5.3 Is there any obligation to notify individuals, including end users of applications, in the case of a data breach?

Jurisdiction	
Hong Kong	As described by the Privacy Commissioner, a data breach is generally taken to be a suspected breach of data security of personal data held by a data user, by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use. The PDPO does not specifically require data users to notify the Privacy Commissioner or affected data subjects in the event of a data breach. However, the Privacy Commissioner has published guidance strongly encouraging data users to make notification when a real risk of harm is reasonably foreseeable. Notification to regulators is also expected if the data user is licensed by the HKMA, the SFC or the IA. In January 2020, the Privacy Commissioner and the government proposed introducing mandatory notification of data breaches to the Privacy Commissioner and affected data subjects if they involve a real risk of significant harm. Other details being considered include a notification time frame and whether to apply a different threshold for notification to data subjects. No concrete legislative amendment proposals have been published and the precise legislative timetable for this mandatory notification requirement to come into force has not been made clear.

Jurisdiction	
China	Under the PIPL, companies are required to implement measures to prevent and address any unauthorised access, or personal information leaks, theft, distortion or deletion (PI breach). In the event of a PI breach, companies are required to take remedial steps and inform affected individuals of the remedial steps taken. The PIPL does not provide a specific timeline for notification of PI breaches. Notification is not necessary if the personal information processor has taken measures to effectively prevent the PI breach from causing harm, unless the competent personal information protection authority considers notification to data subjects is otherwise necessary. In circumstances in which there has been leakage or possible leakage of telecommunications users' personal information, which has caused or may cause "serious" or "severe" consequences, the relevant internet information service provider must make a report to the competent telecommunications regulatory agency. In addition, network operators must take remedial action immediately, inform users and report the issue to relevant authorities upon discovering a security flaw. Networking entities and other organisations may need to make a report to the local public security body within 24 hours of discovering a security breach.
Singapore	In terms of reporting obligations, Part 6A of the PDPA imposes an obligation on organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or Personal Data Protection Commission (PDPC) where it is assessed to be so. Assessments should be done expeditiously as the likelihood of significant harm to affected individuals may increase with time. Any unreasonable delay in assessing a data breach will be a breach of the notification obligation. A data breach which is likely to result in significant harm to an affected individual is notifiable. This includes, for instance, data breaches involving an individual's full name or full national identification number, together with their financial information which is not publicly disclosed or medical information; or an individual's username and password. Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation or public agency, the data intermediary is required to notify the organisation or public agency without undue delay from the time it has credible grounds to believe that the data breach has occurred.
Japan	The amendments implemented in April 2022 include a provision regarding a notification obligation upon leakage, destruction or damage of personal data. Pursuant to that provision, the business operator should notify the PIPC and the data subject of the incident when such incident falls within categories that are likely to harm the rights and interests of individuals under PIPC regulations. Separately, business operators regulated under the Telecommunications Business Act (Act No. 86 of 1984, as amended) (TBA) must report incidents involving the leakage of personal information and the cause of such incidents to the MIAC without delay.

Jurisdiction	
Australia	The Privacy Act introduced the Notifiable Data Breach scheme, which establishes mandatory investigation and notification obligations when there is an "eligible data breach" involving personal information held by an entity covered by the Privacy Act. The data security breach must be an "eligible data breach", meaning: 1. there has been unauthorised access to, or unauthorised disclosure of, information held by an entity; or 2. information has been lost in circumstances where there is likely to have been unauthorised access to or unauthorised disclosure of information; and 3. a reasonable person would conclude that the access or disclosure would likely result in serious harm to any of the individuals to whom the information relates. The serious harm requirement could include physical, psychological, emotional, economic or financial harm. It also covers serious harm to reputation. This is assessed through applying a test of reasonableness in the circumstances. An entity should take into consideration the kind of information accessed and its sensitivity, the kind of person who has obtained the information, whether the information was protected by security measures and whether those measures could be overcome, and the nature of the harm it could cause. Once an entity becomes aware of a breach, they must prepare a statement setting out a description of the data breach, the kinds of information concerned and recommendations about the steps individuals can take in response to the breach. This statement must be provided to the Australian Information Commissioner. The entity must also, as soon as reasonably practicable, take steps to notify the contents of the statement to each of the individuals to whom the relevant information relates, or those individuals who are at risk of the data breach, or publish a copy of the statement on its website and take reasonable steps to publicise the contents of the statement.

5.4 Is there any requirement to register with any national data protection authority? Are there any specific auditing obligations?

Jurisdiction	
Hong Kong	There is no need to register with or notify any authorities of data processing, nor is there any statutory requirement to appoint an official data protection officer. In respect of cross-border transfers of data, this is governed by section 33 of the PDPO. However, despite being promulgated in 1996, this has yet to come into operation nor has there been an indication when it will. Instead, the Privacy Commissioner issued Guidance on Personal Data Protection in Cross-border Data Transfer in December 2014and further guidance on recommended model contractual clauses (RMCs) for transfers of personal data to entities outside Hong Kong in May 2022. The latter applies to a transfer controlled by a Hong Kong data user, providing for two sets of RMCs to cater for data transfers between data users, and between data user and data processor. The RMCs deal with purpose of use, any onward transfer, security, retention, and erasure. Although there are no statutory obligations to conduct an audit, the December 2014 guidance states that in situations where personal data is transferred outside of Hong Kong, regular audit and inspection of the transferees' operations to ascertain their compliance with the requirements under the PDPO (to be provided for in appropriate data transfer agreements) is an effective monitoring tool for adequate and continued protection of personal data.

Jurisdiction	
China	Data may be subject to regulation by the PRC state secret protection department (NASSP) and its local counterparts if such data qualifies as a state secret pursuant to the PRC State Secrets Protection Law. A state secret is defined as a matter that has a vital bearing on state security and national interests, which is only permitted to be disclosed to a limited number of people for a certain period of time. Where an entity is unclear whether or not a matter is a state secret, the entity should make a report to the NASSP or its local counterparts for its review and decision. The PRC's NASSP or its local counterparts have authority to monitor compliance with the PRC State Secrets Protection Law, and entities have an obligation to co-operate with such inspection. Pursuant to the PRC Cybersecurity Law, critical information infrastructure operators (CIIOs) purchasing network products and services are subject to cybersecurity review if such activities may affect national security. New Measures for Cybersecurity Review (the New Measures) came into effect on 15 February 2022. The New Measures were issued by the Cyberspace Administration of China (CAC) jointly with 12 other government departments (together, the Working Mechanism). The New Measures confirm the expanded scope of the cybersecurity review requirement, which now applies not only to CIIOs, but also network platform operators whose data processing activities may affect national security. (The scope had first been proposed to be expanded by draft measures issued in July 2021.) The New Measures refer to "network products and services" as core network equipment, important communications products, high-performance computers or servers, mass storage equipment, large databases or applications, network security equipment, cloud computing services and other network products or services that have an important impact on the security of critical information infrastructure and network and data security. As for the meaning of "data processing", guidance is not provided in the New Measures. In the PRC Data Security Law, data processing is defined as the collection, storage, use, processing, transmission, provision and disclosure of data. Cybersecurity reviews may be initiated by the Working Mechanism. During a cybersecurity review, the national security risk is assessed based on the following main factors: • The risk of critical information infrastructure being illegally controlled, tampered with or sabotaged. • The risk of an interruption in supply endangering the continuity of critical information infrastructure. • The security, openness, transparency, diversity of sources and reliability of supply channels of network products or services, and the risk of supply being interrupted due to political, diplomatic, trade or other factors. • The risk of core data, important data or a large amount of personal information being tampered with, leaked or destroyed, or illegally exported or used. See our **alerter on network security review**. Security assessment for exports of personal information may also be required as discussed under **section 5.1**.

Jurisdiction	
Singapore	There is currently no such requirement under the PDPA for organisations to register with the PDPC. However, there is a requirement for every organisation to appoint at least one data protection officer (DPO), and any of the DPO's business contact information must be made available to the public. Organisations are strongly encouraged to inform the PDPC of the details of their appointed DPO(s) so as to help DPOs keep up with relevant developments in personal data protection in Singapore. While there are no specific auditing obligations in the PDPA, organisations are required to implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity. The PDPC also recommends organisations to undertake a risk assessment exercise to ascertain whether their security arrangements are adequate.
Japan	Registration with the PIPC is not required. There are no audit obligations under the APPI. However, the PIPC Guidelines require regular audits to be conducted, by the party in possession of the personal data, on the data handler who is delegated the task of data handling by the party in possession.
Australia	There is no requirement for entities in Australia that deal with personal data to register with a national data protection authority, nor are there any requirements regulating the auditing of personal data. As outlined in **Section 5.2** requires an entity to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference or loss as well as unauthorised access, modification or disclosure. To ensure compliance, the Office of the Australian Information Commissioner (OAIC) has recommended that entities document their internal practices, procedures and systems. The OAIC's guide to securing personal information recommends that these are regularly reviewed and updated to ensure they reflect current acts and practices.

5.5 Is there any obligation to disclose personal data to government and under what circumstances should personal data be disclosed?

Jurisdiction	
Hong Kong	A number of public authorities and regulators have powers to access or compel disclosure of information. For example: 1. Section 43 of the PDPO provides that the Privacy Commissioner can be provided with any information or document from persons as the Commissioner thinks fit for the purposes of any investigation 2. Section 58 supports law enforcement agencies' (including overseas agencies) and financial regulators' (including the Hong Kong Monetary Authority and the Securities and Futures Commission) powers by facilitating disclosure by data users such as banks (which may disclose under an exemption without the data subject's consent or right to request access to his or her data). For example, the SFC has the power to require production of documents for the purpose of its investigations, which may contain personal data such as a bank customer's account information. Section 58 operates by providing for exemption from Data Protection Principles (DPP) 3 and 6 where personal data is used for the purpose of, and the application of the relevant DPP would likely prejudice, among other things, the prevention or detection of crime; the apprehension, prosecution or detention of offenders; or financial regulators' discharge of specified functions. Crime is defined to include an offence under foreign law where the personal data is to be used in connection with law enforcement co-operation between Hong Kong and a foreign country. DPP 3 provides for the use of personal data only with the data subject's consent; DPP 6 provides for a data subject's right to request access to his or her personal data and to request correction. 3. The Inland Revenue Department can request the name, place of residence and amount of remuneration of any employee from an employer under section 52(2) of the Inland Revenue Ordinance (Cap. 112) 4. Under the Interception of Communications and Surveillance Ordinance (Cap. 589), the Customs and Excise Department, Hong Kong Police Force and the Independent Commission Against Corruption can apply for a prescribed authorisation from a panel judge to intercept any communications in a telecommunications system for the purposes of preventing or detecting serious crime or protecting public security

Jurisdiction	
China	Generally, disclosure of personal data to a third party requires consent from the relevant individual, with a few exceptions, examples being: 1. pursuant to the Criminal Procedure Law, any entity or individual, upon discovering the facts of a crime or criminal suspect, has the right and duty to report the case or provide information to a public security organ, a procuratorate or a court; and 2. pursuant to the Criminal Procedure Law, defence lawyers must promptly inform judicial organs of the information that comes to their knowledge, indicating that their clients or other persons may commit or are committing crimes endangering state security or public security, or crimes seriously threatening the personal safety of others. Under the PRC Personal Information Protection Law (PIPL), relevant regulators have a broad mandate to protect personal information and may require disclosure in the process. For example, the authorities responsible for performing personal information protection functions shall, among other things, (i) require personal information protection assessment in respect of, for example, application programmes; and (ii) investigate illegal personal information processing activities. Pursuant to the Data Security Law (DSL), companies and individuals are required to co-operate with security authorities to give them access to data for the purpose of safeguarding national security or investigating potential crimes. Such a co-operation requirement is not new – the Cybersecurity Law has similar requirements for network operators to provide technical assistance, which may include requests for data access. Furthermore, the Provisions on Internet Security Supervision and Inspection by Public Security Organs give wide inspection and investigation powers to public security organs in respect of Internet security. Irrespective of their industry or place of incorporation, companies doing business in China who fall within the broad definition of internet service providers and network using entities must co-operate in such inspections and investigations. Pursuant to the PRC Intelligence Law, intelligence authorities may request, access or review relevant materials where national security or the public interest may be endangered.
Singapore	The PDPA sets out several circumstances in which personal data may be disclosed without consent, and the following circumstances may apply to allow disclosure to the government or any governmental agency: 1. the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual 2. the disclosure is necessary in the national interest, which can be evidenced by a certificate signed by a Minister 3. the disclosure is necessary for any investigation or proceedings 4. the disclosure is to a public agency and such disclosure is necessary in the public interest 5. the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer
Japan	Under Article 27 of the APPI, personal information must not be disclosed to a third party without the consent of the relevant individual to which the personal information pertains, save for a number of specified scenarios where consent is not required (such as, for example, where disclosure is mandated pursuant to the requirements of any applicable law or regulation).

Jurisdiction	
Australia	APP 6 outlines that personal information may only be used or disclosed for a purpose for which it was collected (known as the 'primary purpose'), unless an exception applies. APP 6.2(b) outlines an exception that allows for the use or disclosure of personal information when required or authorised by or under an Australian law or a court/tribunal order. This may, for example, include situations where: 1. a warrant, order or notice is issued by the court to produce records or information held by the entity; 2. there is a statutory requirement to report certain matters to an enforcement body (e.g., suspected cases of child abuse or specific financial transactions); or 3. a law applying to the entity clearly and specifically authorises the use or disclosure of such information. APP 6.2(e) outlines another exception that allows for the use or disclosure of personal information when the entity believes this is reasonably necessary for one or more enforcement-related activities conducted by, or on behalf of, a Commonwealth, State or Territory enforcement body. Enforcement-related activities include the prevention, detection, investigation and prosecution or punishment of criminal offences, and intelligence gathering activities.

Data Protection and Cybersecurity Trends to Watch

Access to data and certain technologies is crucial to innovation and everyday operations, so businesses' investment in technology and tech talent will continue, while regulators will be seeking to address risks arising from the growing importance and market power of "Big Data" and "Big Tech".

- For many companies, personal data has become one of their greatest assets and yet one of their biggest potential liabilities. Data-related enforcement will remain a key risk as data protection and cybersecurity laws will be more assertively enforced, particularly for egregious breaches of these laws.
- With data matters often also engaging wider issues, such as risk control and operational resilience, the trend of multiple regulators investigating breaches will continue, prompting many companies to refine their breach response and regulatory interaction strategies, particularly where they have sectoral regulators.
- In the civil courts, judges will continue to scrutinise claims where data subjects have not suffered material harm. Stand-alone litigation related to more serious data breaches will continue to be a focus for claimant firms and third-party funders.

- We will see a growing number of privacy and cybersecurity laws coming into force, with the EU's Cyber Resilience Act, updates to the EU's Network and Information Security Directive, and a US federal privacy law and various state laws among the expected new cohort, as well as possible amendments to the UK's data protection legislative framework post Brexit. We will also see guidance and implementing regulations being issued which will further develop the application of existing laws, including China's Personal Information Protection Law, Cybersecurity Law and Data Security Law.
- Companies managing increasingly complex and fragmented data protection compliance programmes will be paying particular attention to developments in international data transfer, sensitive data processing, targeted advertising, data monetisation, self-sovereign identity, IoT and ransomware attack response, and as market practice evolves following developments in regulations, guidance and case law in these areas.

For more information, see our publications **US Lawmakers Release Draft of Comprehensive Federal Data Privacy Bill**; **Digital Services Regulation in the EU: An Evolving Landscape**; **An Overview of the Newly Adopted EU Data Governance Act**; **The Data Act: A Proposed New Framework for Data Access and Porting Within the EU**; **E-Privacy Check-In: Where We Are, and Where We're Headed – Are We any Closer to EU Institutions Reaching an Agreement on the Final Regulation Text**; **UK International Data Transfer Agreement and UK Addendum to the EU Standard Contractual Clauses Laid Before Parliament**; **UK Data Reform: Evolution not Revolution**; **Lloyd v Google: How the Supreme Court Judgment Closed the Door on Lloyd's £3.3bn Data Claim**; **Instagram hit with Historic GDPR Fine: EU Privacy Watchdog urges companies to "Leave Them Kids Alone"**; **One "Fine" Day? Insights from the First Fine issued by the California Attorney General under the California Consumer Privacy Act**; **Australian Privacy Commissioner's Case Against Facebook to Carry On: Facebook Found to be 'Carrying on Business' in Australia**; **Google LLC Ordered to Pay an AUS$60m Penalty for Misleading Users about the Use and Collection of their Personal Location Data**; and **Cyber on ASIC's Mind: AFS Licensees told to Manage Cyber Risk Adequately or face Enforcement Action**.

CYBERSECURITY

6. CYBERSECURITY

6.1 Are there particular laws or codes of practice specifically regulating cybersecurity?

Jurisdiction	
Hong Kong	There is no overarching legal framework for cybersecurity in Hong Kong. The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) addresses the requirement for security of personal data, including data storage and security measures. The Office of the Privacy Commissioner for Personal Data (the Privacy Commissioner) is an independent statutory body set up to oversee the enforcement of the PDPO. That said, in May 2022, the Hong Kong government indicated that it is considering legislation defining the cybersecurity obligations of critical infrastructure operators; public consultation on this will begin by the end of 2022. **Cybersecurity-related crimes** There are a number of offences under Hong Kong law targeting cybersecurity-related crimes, including but not limited to: a. **offences involving data disclosure without consent** – obtaining personal data without consent and disclosing that personal data with an intent to obtain gain or cause loss in money or other property, or disclosure of personal data without consent with an intent (or being reckless) to cause specified harm, the latter offence targeting doxing (section 64 of the PDPO) b. **offences involving hacking** – unauthorised access via telecommunications to a program or data held in a computer (section 27A of the Telecommunications Ordinance) (Cap. 106) c. **computer access offence covering hacking, phishing and DoS attacks** – access to a computer with intent to commit an offence, with dishonest intent to deceive or cause loss, or with a view to dishonest gain (section 161 of the Crimes Ordinance) (Cap. 200). This offence would cover: • hacking; • phishing (social engineering or interaction whereby the phisher masquerades as a legitimate entity to trick the victim into revealing personal or sensitive information or infect the victim's machine with malware); and • a denial of service (DoS) attack, which seeks to make a machine or network unavailable to its intended users by flooding the targeted network server or host with traffic, subject to the involvement of access to another's computer. According to a 2019 Court of Final Appeal case, the section 161 offence is not triggered if only a person's own computer is employed. On the facts, primary school teachers using their own smartphones to take photographs of the school's admission interview questions and disseminating the same to third parties was held not to be caught by section 161. d. **criminal destruction or damage to property** (or a threat of the same) including by way of misuse of a computer (sections 59 to 61 of the Crimes Ordinance); this would cover infection with malware, as well as a DoS attack e. **burglary** (section 11 of the Theft Ordinance) (Cap. 210) – entering any building as a trespasser with the intent to do unlawful damage to a computer or computer storage medium, or program or data held in the same f. **theft of property** (includes intangible property such as digital or electronic data or files) (sections 2 to 9 of the Theft Ordinance)

Jurisdiction	
	g. **fraud** (section 16A of the Theft Ordinance) – inducing another to commit an act or make an omission by deceit and with intent to defraud; this may occur online h. **blackmail** – the use of ransomware may constitute blackmail (section 23 of the Theft Ordinance) i. **money laundering** – if a ransom is paid, the victim will have reasonable grounds to believe or even know that the ransom payment represents the cyber-attacker's proceeds of an indictable offence (section 25 of the Organised and Serious Crimes Ordinance, which is the money laundering offence in Hong Kong) (Cap. 455) (OSCO); a defence is available if the victim notifies an authorised officer, including a police officer, of the payment (whether in advance and obtains consent, or as soon as reasonable thereafter) (section 25A of OSCO) In July 2022, the Law Reform Commission published a consultation paper recommending a new single ordinance to deal specifically with cybercrime and the introduction of five cybercrimes into Hong Kong law comprising: illegal access to a program or data; illegal interception of computer data; illegal interference with computer data; illegal interference with a computer system; and making available or possessing a device or data for committing a crime. This would bring Hong Kong in line with the position globally. The breadth of existing law is proposed to be retained with some existing offences refined and consolidated into the recommended new ordinance. Extraterritorial application is suggested in cases where there is a connection with Hong Kong and serious damage to Hong Kong may be caused. Views on the availability of defences and exemptions were sought; the consultation period ended on 19 October 2022. **Personal Data (Privacy) Ordinance** The PDPO requires all practicable steps to be taken to ensure that personal data held by a data user is protected against unauthorised or accidental access, processing, erasure, loss or use (Data Protection Principle (DPP) 4(1)). Guidance for DPP 4 and its compliance, as well as corporate governance and cybersecurity, is contained in: a. Guidance for Data Users on the Collection and Use of Personal Data through the Internet (April 2014) b. General Reference Guide – Privacy Management Programme (PMP) Manual for the Private Sector (updated in March 2019) c. Guide to Data Protection by Design for Information and Communications Technology (ICT) Systems (May 2019) d. Guidance Note on Data Security Measures for ICT (August 2022) The PDPO does not require that personal data security breaches be notified. However, whilst not a legal requirement, the Privacy Commissioner does encourage notification of breaches, and has issued the Guidance on Data Breach Handling and Giving of Breach Notifications (January 2019). In January 2020, a paper was published by the Constitutional Affairs Bureau (for discussion in the relevant Legislative Council panel) proposing that data breaches be notified to the Privacy Commissioner and the relevant data subjects if they involve a "real risk of significant harm". No concrete legislative amendment proposals have been published and the precise legislative timetable for this mandatory notification requirement to come into force has not been made clear.

Jurisdiction	
	HKMA and HKAB initiatives and guidance Hong Kong Monetary Authority (HKMA) Cybersecurity Fortification Initiative (CFI). Financial regulators in Hong Kong are showing an increased focus on cybersecurity, demonstrated by the HKMA's launch of the CFI in 2016. The CFI aims to strengthen banks' cyber resilience in the areas of governance; identification of cyber-attackers' tactics and techniques; protection through access control, system and device protection and Application Programming Interface (API) testing; third-party risk management; and cyber risk management and cyber incident detection, response and recovery. An upgrade (CFI 2.0) was announced in November 2020, reflecting the latest developments in sound cyber practices overseas. One pillar of the initiative is the Cyber Resilience Assessment Framework (C-RAF), which is for banks to assess their own cyber risk exposure, and required cybersecurity controls. Banks have been divided into three groups and there is a timeline for the three groups to complete their C-RAF 2.0 assessments, starting 2021 through 2023. This followed a holistic review of the CFI including C-RAF with the results showing that 90% of banks found C-RAF to be useful, especially in identifying previously unrecognised gaps. C-RAF comprises three components: inherent risk assessment, maturity assessment and the intelligence-led Cyber-Attack Simulation Testing (iCAST) exercise. Banks found iCAST helpful in preparing for cyber-attacks, albeit it is only applicable to banks with an inherent risk level assessed at medium or high. Another part of the CFI initiative is a channel to facilitate cyber intelligence exchange between banks, known as the Cyber Intelligence Sharing Platform (CISP), which helps in preparing for possible cyber-attacks and enhancing resilience. **Cybersecurity.** The HKMA issued various cybersecurity-related circulars concerning cyber risk management and oversight, contingency planning, data security and cyber resilience in October 2014 and September 2015. These require banks to comply with the PDPO and implement layers of both IT and non-IT security controls to protect systems and networks, prevent or detect loss or leakage of customer data, and to have in place effective incident handling and reporting procedures. To assist banks with understanding and complying with the PDPO, the Privacy Commissioner has issued Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry. It has also issued the Ethical Accountability Framework for the collection and use of personal data in the online environment, which the HKMA encourages banks to adopt. In addition, the HKMA has issued a number of Supervisory Policy Manual modules relating to cybersecurity issues including those covering General Principles for Technology Risk Management, Risk Management of E-banking, Operational Resilience and Business Continuity Planning. More recently, the Risk Management of E-banking module has been cited in the Sound Practices for Customer Data Protection circular of April 2022, which was issued following a thematic examination. The circular shares four areas of sound practices, namely, customer data governance frameworks defining the roles and responsibilities of data owners and endorsed and overseen by the board and senior management; data inventory identification, review and management; controls over the transmission and storage of data; and physical and logical security controls over data. Cybercrime is a concern as illustrated by the circular issued by the HKMA in October 2021 regarding Authentication and Fraud Prevention Controls for Simplified Electronic Direct Debit Authorisation (pre-authorisation of direct debit payments is provided for as part of the Hong Kong Faster Payment System). Good practices are set out for authentication of the customer's identity and verification of the customer's personal and account information including two-factor authentication, default transaction and daily limits, and SMS notification. Similar good practices were set out in an earlier circular in May 2016 regarding Security Controls related to Internet Banking Services, having regard to incidents of unauthorised share trading transactions at the time. The General Principles for Technology Risk

Jurisdiction	
	Management, Operational Resilience and Business Continuity Planning Supervisory Policy Manual modules are cited in the Sound Practices for Payment Operations circular of July 2022, which discusses another aspect of cybersecurity, that of the preparedness to deal with IT system malfunctions and outages, as well as service degradation. The July 2022 circular emphasises the need for a robust business continuity plan and high operational resilience with respect to payment operations, which are critical in nature. **Third-party service providers and back-up.** The Code of Banking Practice, a non-statutory code issued by the Hong Kong Association of Banks (HKAB), also emphasises the need for banks to have in place appropriate control mechanisms to protect customers' data. It highlights the fact that banks remain accountable for data transferred to a third-party service provider and should adopt contractual or other means to safeguard data. In May 2021, the HKMA requested banks to critically assess the need for setting up secure tertiary data back-up (STDB) to counter the risk of destructive cyber-attacks having regard to their risk exposure and the principles stipulated in the HKAB STDB Guideline. The HKMA has also recognised the growing trend of banks adopting cloud computing via the engagement of third-party cloud service providers (CSPs) for not only basic and non-core operations, but also more important ones. Following similar themes, it set out its supervisory expectations in this area in a circular in August 2022 including effective controls to ensure the security of banks' information assets, a viable and effective contingency plan to cope with disruption, and a clear and enforceable CSP engagement agreement to protect banks' interests, risk management needs and ability to comply with supervisory expectations. **Regtech.** To promote the use of regtech in the area of cyber defence, the HKMA shared use cases with the banking industry in the first edition of Regtech Watch (in November 2019) including behavioural biometric techniques for user authentication; artificial intelligence to analyse activity logs to detect abnormal activities indicating cyber-attacks; and robotic process automation to automate routine tasks such as system access assignment, system security setting and security testing. **SFC guidance and enforcement** **Internet trading.** In October 2017, following a consultation, the SFC published the Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading (Internet Trading Guidelines). These set out baseline cybersecurity requirements for those offering Internet trading services covering preventive, detection and internal governance-related controls. One key control, the implementation of two-factor authentication (2FA) for clients to log in to their Internet trading accounts, took effect on 27 April 2018, while all other requirements took effect on 27 July 2018. At the same time, and supplementing the Internet Trading Guidelines, the SFC issued a Circular to Licensed Corporations Engaged in Internet Trading regarding Good Industry Practices for IT Risk Management and Cybersecurity, which advised that the Internet Trading Guidelines are only minimum standards and senior management should ensure that all cybersecurity controls are commensurate with business needs and operations, and implement additional controls as necessary. The circular contains a list of good cybersecurity practices for consideration. In September 2020, the SFC followed up with a report after conducting a survey of 55 Internet brokers and onsite inspections of 10 of them. The findings revealed that most firms complied with the SFC's key regulatory requirements, but there were deficiencies in the protection of clients' Internet trading accounts (including in the implementation of 2FA, data encryption, and monitoring and surveillance to identify suspicious unauthorised transactions); infrastructure security, and user access management, as well as cybersecurity management and incident reporting. Firms were reminded to comply with the Internet Trading Guidelines and encouraged to implement good practices.

Jurisdiction	
	Instant messaging orders. Other than Internet trading, clients may be permitted to make orders through instant messaging, but adequate controls must be in place to ensure compliance with statutory and regulatory requirements including the keeping of proper records. The SFC issued a circular in this regard in May 2018 regarding the measures to be implemented in the areas of centralised management of order messages and associated accounts, and devices for record-keeping and compliance monitoring to detect questionable transactions; security and reliability including authentication of client identities, safeguards against unauthorised access and security attack, and contingency planning; written internal policies and procedures, and training; and client awareness of risks and terms and conditions. **External electronic data storage.** In relation to regulatory records maintained using external electronic data storage services, a licensed corporation should designate at least two individuals, being Managers In Charge of Core Functions (MICs), in Hong Kong, who will be responsible for ensuring information security to prevent unauthorised access, tampering with or the destruction of regulatory records. For more, **see our RIFC blog post regarding the circular on the use of external electronic data storage**. **Business continuity planning and operational resilience.** Similar to HKMA requirements, under the Management, Supervision and Internal Control Guidelines of the SFC, firms are required to implement an effective business continuity plan appropriate to their size to ensure that they are protected from the interruption risk that may arise from a cyber-attack. Key processes include: a business impact study, identification of likely scenarios involving interruptions (e.g., breakdown of data processing systems), and regular testing of the firm's disaster recovery plan. In May 2017, a new variant of ransomware, namely, WannaCry, spread over the Internet, which prompted the SFC to issue a circular reminding licensed corporations to be alert to cybersecurity threats and critically review and assess the effectiveness of their cybersecurity controls, and setting out a list of preventive measures to be considered. Operational resilience has received renewed attention in light of COVID-19 and remote working. In September 2020, the SFC issued a circular reminding licensed corporations to assess their operational capabilities and remote office arrangements, and implement appropriate measures to manage the associated cybersecurity risks. It set out examples of controls to protect internal networks and data where remote access measures such as virtual private networks and videoconferencing are used. In October 2021, with the transition of many intermediaries to hybrid working and considering the maintenance of the same as a new normal, the SFC issued a further circular providing for operational resilience standards and required implementation measures generally in the areas of governance; operational risk management; information and communication technology systems; third-party dependency risk management; and business continuity planning and incident management. The circular also sets out expected regulatory standards for managing remote working risks, sharing lessons learned drawn from the SFC's review of some licensed corporation's operational resilience measures during the pandemic and suggesting techniques for mitigating remote working risk.

Jurisdiction	
	Disciplinary actions. The importance of ensuring protection from cyber-attacks and incidents resulting in data breaches includes the fact that they may be seized on by financial regulators in determining whether sufficient controls are in place, and of regulatees' fitness and propriety. Examples of SFC enforcement involving a data breach include the September 2018 disciplining of Mr Ngo Wing Chun, a former relationship manager of The Hongkong and Shanghai Banking Corporation (HSBC), who sent an email containing the personal data of nearly 1,000 customers to his personal email accounts on his last working day at HSBC. The customer data leakage was detected by HSBC's email monitoring system the following day. Mr Ngo was banned from re-entering the industry for 12 months. In similar incidents in January 2018 and June 2017, former employees were banned from re-entering the industry for six and eight months, respectively, for transferring client personal data prior to their departure. Whilst not involving a data breach, Ms Mo Shau Wah, a former account executive of China Pacific Securities Limited (China Pacific), was banned from re-entering the industry for life in March 2020 following her criminal conviction for stealing shares from China Pacific's clients and making unauthorised sales of stolen shares through nominee client accounts in the name of her relatives. The theft was covered up through false entries in the computer system and client statements.
China	The Cybersecurity Law of the People's Republic of China took effect on 1 June 2017. The Cybersecurity Law applies to critical information infrastructure operators (CIIOs) and network operators and requires them to fulfil certain security protection obligations including to (i) develop internal security management rules and operating procedures, as well as designate persons in charge of cybersecurity; (ii) take technical measures to prevent computer viruses, network attacks and other acts that endanger cybersecurity; (iii) take technical measures to monitor and record the status of network operation and cybersecurity incidents and preserve weblogs for not less than six months; and (iv) take data categorisation measures, and back-up and encrypt important data. CIIOs are required to fulfil additional security protection obligations including (a) establishing a designated security management department, designating persons in charge of security management, and carrying out background checks of the persons in charge and personnel in key positions; (b) arranging regular cybersecurity education, technical training and skill assessment for employees; (c) preparing disaster recovery back-up of important systems and databases; and (d) formulating emergency response plans for cybersecurity incidents, and organising drills on a periodic basis. Other rules and regulations governing cybersecurity have since been issued and include the following: 1. The Cloud Computing Services Security Assessment Measures, which govern the security of cloud services and the security assessment conducted by government authorities over cloud service providers. 2. The Provisions on Administration of Security Vulnerability of Network Products, which set out the requirements for discovery, reporting and and repairing of vulnerabilities in network products applicable to network product providers and network operators.

Jurisdiction	
Singapore	On 5 February 2018, Singapore passed a Cybersecurity Act to, inter alia, require or authorise the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, and to regulate the owners of critical information infrastructure. On 20 September 2021, the Cyber Security Agency of Singapore (CSA) sought industry feedback on a proposed licensing framework for cybersecurity service providers (CSP), which became operative in April 2022. This is a light-touch licensing framework that only applies to two types of services. First, to penetration testing services, which check if an organisation can identify and respond to simulated cybersecurity attacks. Secondly, to services that monitor activities in computer systems to identify threats. There are two main licensing requirements CSPs must comply with. First, it must ensure its key officers are fit and proper. This entails showing that a key officer does not have criminal convictions or judgments entered against him or her for fraud, dishonesty or moral turpitude. Secondly, licensed CSPs are required to retain for three years basic records on cybersecurity services it has provided. As a corollary of the first requirement above, licensed CSPs are required to notify the CSA at least 30 days before the appointment of a new key officer. Further, it must notify the CSA where a key officer ceases to hold office, there are inaccuracies in his or her particulars, or criminal convictions/judgments have been entered against him or her. To protect consumers of cybersecurity services, licensees must also comply with professional conduct requirements. These include: • not making false representations in advertisements or in providing its services; • complying with applicable laws such as the Computer Misuse Act and all obligations relating to confidentiality and data protection; • exercising due care and skill and acting with honesty and integrity; • not acting in a manner that brings about conflicts of interests; and • collecting, using or disclosing information only for the purposes of providing its cybersecurity services. The licensed CSPs must provide information concerning its cybersecurity services upon request to assist the CSA in its investigations. The licences are valid for two years. The registration fee payable for business entities is S$1000, while for individuals (e.g., freelancers or sole proprietorships), it is S$500. However, due to COVID-19, 50% of the fees will be waived for applications lodged within the first 12 months from the commencement of the licensing framework. In addition, there is the Computer Misuse Act, which deals with hackers and similar forms of unauthorised access/modification of computer systems. The Monetary Authority of Singapore (MAS) has issued various notices, guidelines and circulars in respect of cybersecurity, including a notice requiring financial institutions to notify MAS as soon as possible, but not later than one hour following, the discovery of a serious cybersecurity incident. The MAS has also issued guidelines comprising industry best practices that financial institutions are expected to adopt, and which have some relevance to cybersecurity. Whilst the guidelines are not legally binding, the degree of observance with the spirit of the guidelines by a financial institution is an area of consideration by regulators in assessing the risk of the financial institution.

Jurisdiction	
Japan	Regulation The Basic Act on Cybersecurity (Act No. 104 of 2014, as amended) (Cybersecurity Act) regulates how the government, various types of business entities and educational research organisations must act to ensure cybersecurity. Also, the Penal Code (Act No. 45 of 1907, as amended) and the Act on Prohibition of Unauthorized Computer Access (Act No. 128 of 1999, as amended) prescribe punishments for hacking activities and other unauthorised computer access. The Cybersecurity Act provides an outline of the potential regulations. However, specific regulations are not provided. Instead, supervising authorities in each sector often establish specific regulations. For example, the Financial Services Agency of Japan has established guidelines to avoid certain types of cyber-attacks (such as the Comprehensive Guidelines for Supervision of Major Banks, etc.) and requires regulated entities (e.g., banks) to establish and maintain compliance systems, including information security systems (such as maintaining clients' important information) and security systems targeted at preventing cyber-attacks (and to establish reporting systems and supervising systems to ward off cyber-attacks). More recently, in 2021, the Basic Act for the Formation of a Digital Society (the Digital Society Act) came into effect and the Digital Agency of Japan (JDA) was established for the purpose of enhancing digital-related regulations. The Digital Society Act provides general principles of the JDA and emphasises the importance of maintaining cybersecurity. An internet service provider is required to be registered as a telecommunications business operator under the Telecommunications Business Act (Act No. 86 of 1984, as amended). Internet service providers are supervised by the Ministry of Internal Affairs and Communications (the MIAC). The Telecommunications Business Act provides for general rules, while the specific regulations are set by the MIAC. Remedies for Breach An entity injured by hacking activities or other unauthorised computer access may claim for damages against the person who performs the activities under the Civil Code. Also, the injured entity may file a complaint with the investigating authorities to prosecute the perpetrator under the Code of Criminal Procedure (Act No. 131 of 1948, as amended), even if the injured entity does not know the identity of the perpetrator. Under the Unfair Competition Prevention Act, an injured party may claim for damages and/or an injunction against a person or entity, if such person or entity acquires, holds or uses a domain name, which is the same as or similar to a name associated with the goods or services of the injured party, for the purpose of wrongful gain or causing damage to other persons/entities.

Jurisdiction	
Australia	Australia does not have a single cybersecurity law. Instead, there is a patchwork of laws and regulatory standards governing cybersecurity, such as: 1. Privacy Act 1988 (Cth): As previously outlined in section 5, this Act imposes a range of obligations in relation to the handling of personal information. This Act also establishes the Notifiable Data Breach scheme, which imposes investigation and notification obligations where there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity that is likely to result in serious harm to any of the individuals to whom the information relates. 2. Corporations Act 2001 (Cth): This Act imposes duties on directors of companies, including a duty to exercise their powers and discharge their duties with the degree of care and diligence that a reasonable person would exercise in the circumstances. The Australian Securities and Investments Commission has indicated that this duty extends to managing cybersecurity risks. Other relevant obligations under this Act include obligations for: • listed entities to disclose information that might reasonably be expected to materially affect the price or value of securities of the entity, which could include information relating to a cyber incident; and • Australian financial services (AFS) licensees to have adequate resources (including financial, technological and human resources) to provide the financial services covered by the AFS licence and have adequate risk management systems in place, which could include adequate cybersecurity measures. As part of this, AFS licensees are expected to identify and evaluate the risks they face (such as cyber risks) with a focus on risks that adversely affect financial consumers or market integrity and regularly review the adequacy of their technological resources, including IT system security, disaster recovery systems and business resumption capacity. 3. Criminal Code Act 1995 (Cth): This Act establishes offences consistent with those required by the Council of Europe Convention on Cybercrime. The offences include unauthorised access to, or modification of, restricted data (i.e., hacking); unauthorised impairment of electronic communication (i.e., denial-of-service attacks); and unauthorised impairment of data held on a computer disk (i.e., infection of IT systems with malware). 4. Cybercrime Act 2001 (Cth): This Act criminalises computer and internet-related offences, such as unlawful access and computer trespass. The Act also establishes investigation powers and criminal offences designed to protect security, reliability and integrity of computer data and electronic communication. 5. Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act): This Act seeks to strengthen the Australian Government's ability to respond to national security threats, particularly sabotage, espionage and coercion, that may be brought about by cyber-attacks. The Act, which currently covers assets in the electricity, gas, water and ports sectors, establishes: • a Register of Critical Infrastructure Assets; • Government information-gathering power with respect to these assets; and • Ministerial directions powers allowing the relevant Minister to issue directions to owners or operators of these critical assets in order to mitigate national security risks.

Jurisdiction	
	In December 2020, the Security Legislation Amendment (Critical Infrastructure) Bill 2020, which would amend the SOCI Act, was introduced into Parliament. This Bill aimed to increase the security and resilience of Australia's critical infrastructure and give effect to an "enhanced regulatory framework" by: • expanding the range of sectors covered by the SOCI Act; • introducing a positive security obligation that will apply to all critical infrastructure entities and consist of a principles-based set of security outcomes and sector-specific guidance and requirements to be designed by entities in conjunction with the relevant regulator in each sector; • introducing additional enhanced cybersecurity obligations for entities involved with infrastructure that is considered to be particularly critical and of national significance, including cybersecurity exercises, incident response plans and vulnerability assessments; and • facilitating government assistance or intervention if necessary to effectively respond to and manage cyber-attacks on the networks and systems of critical infrastructure entities. Following initial consultation, the Australian Government reported that there is broad in-principle support for the reform framework and that it was committed to working with industry to design sector-specific requirements throughout 2021. The Australian Government subsequently split the original Bill into two separate Bills, with both Bills having now been passed by Parliament. This allowed Parliament to promptly legislate pressing reforms in the first Bill and, at the same time, give the Australian Government and relevant industries adequate time to further deliberate the less urgent elements of the original Bill in the second Bill. Under the first Bill, some of the key amendments include: • expanding the range of sectors covered by the SOCI Act to include 11 additional sectors of the economy, namely the communications, data storage or processing, financial services and markets, water and sewerage, energy, healthcare and medical, higher education and research, food and grocery, transport, space technology and defence industry sectors; • expanding the number of entities required to provide information to be recorded on the Register of Critical Infrastructure Assets; • enforcing mandatory cyber incident reporting to the Australian Cybersecurity Centre relating to critical infrastructure assets; and • introducing government assistance and intervention powers to respond to serious cybersecurity incidents. Under the second Bill, some of the key amendments include: • requiring that specified critical infrastructure assets adopt and maintain a critical infrastructure risk management programme; • introducing enhanced cybersecurity obligations that apply in relation to 'systems of national significance', being assets declared by the relevant Minister as having the highest criticality; and • amending provisions that authorise the use and disclosure of protected information to facilitate greater information sharing between regulated entities and regulatory agencies.

Jurisdiction	
	6. Prudential Standard CPS 234 (Information Security): This Standard aims to ensure that entities regulated by the Australian Prudential Regulation Authority (APRA) (including authorised deposit-taking institutions, general insurers, life insurers, private health insurers, licensees of registrable superannuation entities and authorised or registered non-operating holding companies) are resilient against cyber-attacks and other information security incidents. Under the Standard, APRA-regulated entities are required to: • clearly define the information security-related roles and responsibilities of the Board, senior management, governing bodies and other individuals; • maintain information security capabilities commensurate with the size and extent of threats to the entity's information assets, and which enables the continued sound operation of the entity; • implement controls to protect its information assets commensurate with the importance and sensitivity of those information assets and undertake systematic testing and assurance regarding the effectiveness of those controls; • maintain plans to respond to information security incidents that the entity considers could plausibly occur (information security response plans), to be reviewed and tested annually; and • promptly notify APRA of information security incidents. Other relevant APRA standards and guidelines include: • APRA's Prudential Standards – CPS 220 (Risk Management) and CPS 231 (Outsourcing): These Standards require APRA-regulated entities to have proper risk management strategies, including IT systems, and to ensure that they properly manage outsourcing risk in relation to material business activities. • APRA Prudential Practice Guides – CPG 234 (Management of Security Risk in Information and IT) and CPG 235 (Managing Data Risk): These Guides provide guidance to senior management and risk management and technical specialists (both management and operational) about data and security risks and specifically target areas where APRA continues to identify weaknesses as part of its ongoing and supervisory activities. • APRA Information Paper – Outsourcing involving Cloud Computing Services: This Paper outlines prudential considerations and key principles that should be considered when adopting the use of cloud computing services. The Australian Government has also introduced a number of policy measures in relation to cybersecurity, including: 1. **Australia's Cybersecurity Strategy:** This 10-year Strategy, which involves an AU$1.67 billion investment in cybersecurity initiatives, has been introduced with the stated aim of creating "*a more secure online world for Australians, their businesses and the essential services upon which we all depend*". Central to the Strategy is the need for governments, businesses and the community to work collaboratively in order to achieve effective cybersecurity. Some of the key initiatives outlined in the Strategy include: • strengthening the critical infrastructure regulatory framework; • considering the introduction of new laws that establish a minimum cybersecurity baseline across the entire economy which could result in changes to privacy, consumer and data protection laws as well as the duties of company directors;

Jurisdiction	
	• developing new powers accompanied by appropriate safeguards that allow the governments to take action against sophisticated cyber-attacks; and • releasing the "Code of Practice: Securing the Internet of Things for Consumers", a voluntary Code of Practice containing 13 principles to inform businesses of the cybersecurity features expected of internet-connected devices available. 2. **Ransomware Action Plan:** This Plan outlines the initiatives that have already been undertaken by the Australian Government to strengthen cybersecurity together with forthcoming legislative, policy and operational reforms aimed at disrupting and deterring ransomware attacks to better protect individuals, businesses and critical infrastructure across Australia. The Plan also clearly sets out the Australian Government's policy position regarding the payment of ransoms, namely that the Australian Government does not condone the payment of ransoms. Some of the key legislative, policy and operational responses to ransomware attacks outlined in the Plan include: • introducing specific mandatory ransomware incident reporting to the Australian Government; • introducing a stand-alone offence for all forms of cyber extortion; • introducing a stand-alone aggravated offence for cybercriminals seeking to target critical infrastructure; • modernising legislation to ensure that cybercriminals are held to account for their actions, and law enforcement is able to track and seize or freeze their ill-gotten gains; and • establishing a multi-agency taskforce, "Operation Orcus", as Australia's strongest response to the surging ransomware threat, led by the Australian Federal Police. The Plan expresses the Australian Government's intention to work with international counterparts to detect, investigate, disrupt and prosecute malicious cyber actors when engaging in cybercrime and to actively call out those that support or provide safe havens to cybercriminals.

6.2 What rights do I have against hackers and other cybercriminals who may try to gain access to my network?

Victims of cyber fraud may employ a range of civil measures against hackers and cyber fraudsters. Examples of these measures include suing the offender (or internal management) for compensation for the damage suffered from a statutory or regulatory contravention, where available, such as under section 66 of the Hong Kong PDPO or in tort on grounds such as breach of fiduciary duty, breach of confidence, misuse of private information, misrepresentation, fraud and deceit, trespass to chattel, conversion, unjust enrichment, "money had and received", breach of constructive trust, unlawful means conspiracy, dishonest assistance or knowing receipt. Where the cyber fraudster defendants are unknown or refuse to engage in proceedings, which is often the case, freezing injunctions may be obtained against persons unknown; disclosure orders may be obtained, including against innocent third parties mixed up in the wrongdoing, for example, banks into which the funds were deposited, or internet or cloud service providers; and service of legal documents may be by innovative methods, including messaging applications such as WhatsApp and data rooms.

Speedier judgment may be obtained without trial by way of summary judgment, as the fraud exception to summary judgment has been removed in various jurisdictions, such as England since 1992 and Hong Kong since 1 December 2021. If the defendants do not participate in or defend the proceedings at all, default judgment may be obtained.

Enforcement of the judgment may be by way of garnishee proceedings (if the proceeds of the cyber fraud are held in the defendant's / judgment debtor's bank account, the bank is considered to owe the same to the judgment debtor and the court can attach this debt and compel payment to the judgment creditor). Alternatively (albeit uncertainty remains in Hong Kong), the quickest method of enforc ement is to obtain a default judgment, declaration of trust and vesting order at the same time. Whilst this provides for more direct recourse, in that fewer separate applications and hearings are involved and the victim can directly call upon the bank to return traceable proceeds, the availability of a vesting order in the cyber fraud context is subject to conflicting decisions and awaiting appellate guidance, specifically as to the applicability of section 52(1)(e) of the Hong Kong Trustee Ordinance (Cap. 29). Cybercrime victims can also consider suing external service providers for a breach of contract or negligence, depending on the terms and conditions of the service contract and whether the incident is related to a cybersecurity failure on the service provider's part.

In any case, victims of cybercrimes should immediately refer the matter to the police or law enforcement agencies. The police have a special bureau, the Cybersecurity and Technology Crime Bureau, to deal with technology crime. There is a **link for making an e-report**. One point to note is that the 'no consent' regime which previously enabled the police to informally freeze bank accounts dealing with known or suspected proceeds of crime has been found to be unconstitutional. The continuing operation of the 'no consent' regime is uncertain, as the judgment does not provide guidance as to whether – and, if so, how – the regime may be adapted to operate lawfully, and the judgment may be appealed. There may also be legislative change. Nevertheless, cybercrime should still be reported, as it remains the case that the police may inform banks of their suspicions and banks remain obligated not to deal with known or suspected proceeds of crime, and must make suspicious transactions reports. For the purposes of recovery of misappropriated funds, however, accompanying civil action will need to be more seriously considered.

For non-criminal matters, advice on computer security incident response and security protection may be sought from the Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT), which is managed by the Hong Kong Productivity Council. HKCERT has an **incident reporting page**.

6.3 What rights do I have against cybersquatters?

Cybersquatting is generally defined as the registering, sale or use of a domain name containing a trademark to which the registrant does not have the rights, with the intent to profit from the goodwill of the mark. Registering another person's trademark as a domain name may be an act of trademark infringement as well as of passing-off.

"Cybersecurity does not respect borders, and the reputational, financial, and legal impact, as well as loss of customers, from a major cyber-attack may be vast. It is not simply a technology issue. Core policies (data collection / confidentiality / business continuity) must be redesigned with cyber in mind. Company boards must pay attention to cybersecurity risk issues and be able to react quickly."

There are two common routes that can be employed to seek remedy against cybersquatters – court litigation or arbitration. Trademark owners can apply to court for an injunction against such registration and seek compensation for loss suffered as a result of the infringement of intellectual property rights.

For domain name disputes, trademark owners may also consider arbitration as a more cost-effective solution. The Hong Kong International Arbitration Centre is to date the only approved provider of services for mandatory arbitration proceedings for particular Hong Kong domain names (such as .hk). A successful complaint can result in changes, cancellation or transfer of the .hk domain name. The decisions of the arbitrators are binding and there is no appeals process.

6.4 What are the possible risks that may arise from a cyber-attack?

To illustrate the extent of cyber-attack risks, the following table sets out the number of average weekly attacks in May 2021 in the 10 countries in APAC suffering the most attacks in descending order[6]:

Country	Average weekly attacks in May 2021
Indonesia	3,311
Taiwan	2,523
India	1,749
Thailand	1,589
Philippines	1,438
Malaysia	986
Singapore	792
New Zealand	606
Hong Kong	590
South Korea	589

As to whether directors will be prepared to react to the same, according to an Ernst & Young survey, only 9% of boards in 2021 declared themselves extremely confident that the cybersecurity risk mitigation measures presented to them can protect their organisations from major cyber-attacks – down from 20% the previous year.[7] This is reflected in the low funding for cybersecurity: according to another Ernst & Young survey, the average revenue of survey respondents in 2020 was US$11 billion, whilst spending on cybersecurity was on average US$5.3 million per year or about 0.05%. That said, the spending varied across sectors. In the highly regulated financial services and TMT sectors, the average survey respondent spent an average of over US$9.4

6 Check Point Software Technologies Ltd, Asia Pacific experiencing a 168% year-on-year increase in cyber-attacks in May 2021, https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/

7 Ernst & Young Global Ltd, Cybersecurity: How do you rise above the waves of a perfect storm?, 22 July 2021, https://www.ey.com/en_ae/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm

million. On the other hand, energy companies spent an average of just US$2.2 million.[8]

Risks arising from cyber-attacks include potential actions from affected parties which may include employees, customers, third-party suppliers and other vendors.

There is also the risk of actions against senior management or the board of directors, with the cause of action being based on allegations of negligence in failing to take reasonable measures to prevent the attack, or in failing to mitigate the effects of the attack.

On the regulatory side, as cyber-attacks increase around the globe, regulators are responding with new cyber and data laws. New audit and dawn raid powers, and mandatory reporting requirements, are putting businesses in the spotlight. There may be investigations and enquiries with the potential for enforcement actions and sanctions. For more, see our **report on Cybersecurity: What Regulators Are Saying Around the World**.

More specifically as to the risks and legal considerations arising from a ransomware attack, see our **Ransomware: Prevention & Response publication**, which also provides guidance on how to prevent and prepare for a ransomware attack, and what to do if and when a company is the victim of such an attack.

Case Study: Microsoft

On 2 March 2021, Microsoft announced that its Exchange Server software had been attacked by a hacking group referred to as Hafnium. It was reported that the attack allowed unauthorised access to the networks and email systems of at least 30,000 US companies, with some estimating the number of victim companies globally at over 250,000. The European Banking Authority confirmed that its own email servers had been compromised.

According to Microsoft, Hafnium was able to access the Microsoft Exchange Servers of individual organisations by exploiting several zero-day vulnerabilities (previously unknown software vulnerabilities). Once Hafnium obtained access to email servers, it was reportedly able to install malware that allowed it to access and control organisations' wider networks, and steal data.

Microsoft released a software update to remedy the vulnerabilities used by Hafnium. However, industry experts have suggested that Microsoft applied the patch too late and, even after the patch was installed, unauthorised access actors were still able to access victims' networks if they had obtained access prior to installation of the patch.

The wide ramifications of the Microsoft data breach prove that cybersecurity is critical for all businesses with legal and regulatory ramifications and the risk of exposure to liability for cybersecurity failures, including from data-related litigation. For what good, effective crisis management looks like, including in the form of cyber response planning and aftermath management, see our **briefing on Microsoft Data Breach: Risk, Regulation and Managing a Crisis** and our publication **Data Litigation: A Toolkit for Defendants**.

8 Ibid

ANTI-MONEY LAUNDERING

7. ANTI-MONEY LAUNDERING

The price of non-compliance with anti-money laundering (AML) regulations is high, as illustrated by the penalties imposed on financial institutions in APAC. In September 2020, an Australian bank settled with the Australian regulator, Australian Transaction Reports and Analysis Centre (AUSTRAC), to pay a record civil penalty of AU$1.3 billion (approximately US$930 million) for AML breaches related to international transfers through correspondent banks, with the transfers having links to child exploitation.[9] The next month, another record fine was imposed in another jurisdiction, this time by the Hong Kong Securities and Futures Commission (SFC) in the amount of US$350 million for AML control lapses in connection with the 1MDB scandal. (The same financial institution was fined over US$5 billion by regulators in five countries, including the SFC and Monetary Authority of Singapore in 2020.[10]) The People's Bank of China tripled its fines in 2020 totalling some US$87 million compared to 2019 for breaches of AML requirements.[11]

In Singapore, the MAS imposed a penalty of S$1 million on a private bank for its failures to comply with MAS's AML/CFT requirements. There were material lapses in its customer onboarding and ongoing monitoring of business relations with customers.

The adoption of regulatory technology (regtech) is an important part of the AML toolkit. According to a survey by LexisNexis Risk Solutions, this is reflected by the distribution of AML spend in APAC, with financial institutions spending the most on labour and training as a proportion of overall AML spend (50%) with the next highest spend category being technology (at 41%).[12]

"There is no one-size-fits-all when it comes to money laundering controls. Finding the right balance in a risk-based fashion, between practicality and cost-effectiveness, and detecting ML, is a constant challenge. The use of technology is an important tool in striking that balance."

Jonathan Wong, Partner

9 AUSTRAC media release, 24 September 2020
10 finews.asia article, 23 October 2020
11 Nikkei Asia, China threatens money launderers with higher fines, 3 June 2021, https://asia.nikkei.com/Spotlight/Caixin/China-threatens-money-launderers-with-higher-fines
12 LexisNexis Risk Solutions, 2022 Asia Pacific True Cost of Financial Crime Compliance Study, https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-apac

7.1 Do the anti-money laundering (AML) laws of your jurisdiction mandate the use of specific technologies to perform AML compliance functions such as customer due diligence and transaction monitoring? If yes, what are these?

Jurisdiction	
Hong Kong	No. There are general recommendations and guidelines by regulators such as the Hong Kong Monetary Authority (HKMA) and the Securities and Futures Commission (SFC), but no specific technologies have been mandated. **Risk-based approach for AML programme and tech adoption** Significant autonomy is given to regulated financial institutions in terms of design and implementation of their AML compliance programmes. There is no "one-size-fits-all" when it comes to money laundering (ML) controls. Finding the right balance in a risk-based fashion, between practicality and cost-effectiveness, and detecting ML, is a constant challenge. The use of technology, notably data analytics and appropriate integration of external data, in an important tool in striking that balance. In April 2021, the HKMA provided guidance on good practices following its thematic review of banks' use of external data. Key points from the HKMA's guidance include taking a risk-based approach that involves considering the appropriateness of the AML programme's typologies, areas of focus and processes, which should be commensurate with the financial institution's size, services offering, customer profile and geographical footprint. The HKMA observed that technology in the form of data and network analytics, combined with appropriate integration of external data – such as from the Fraud and ML Intelligence Taskforce (a collaboration with the Hong Kong Police Force for information sharing) – has been used effectively in identifying high-risk relationships and suspicious transactions, including mule account networks (i.e., linked accounts that are not genuine customer accounts and potentially used for ML). The importance of senior management support, intelligence sharing within the institution and any wider group, and performance evaluation of the use of data analytics and external data in an AML compliance programme were also emphasised. **Tech adoption in remote customer onboarding** In October 2018, following a consultation, the SFC allowed licensed corporations to adopt supplementary measures, including appropriate technology where customers are not physically present for identification purposes. It declined, however, to prescribe specific examples of appropriate technology to minimise the frequency and extent of revisions necessitated by anticipated rapid developments. Similarly, in its AML FAQs, the SFC declined to prescribe specific technology, but did state that reliable technology solutions may be used to translate documents in foreign languages evidencing a client's identity. In June 2019, it relaxed the approach for the online onboarding of overseas individual clients. The HKMA has also issued guidance for the remote onboarding of customers, including corporate customers in February and August 2019, as well as September 2020. This allows banks to employ appropriate technology solutions to mitigate the risks when identifying and verifying the identity of an individual customer, corporate representative or beneficial owner, and expects that any technology solutions adopted should be at least as robust as those performed when the individual is in front of the staff of a bank. In June 2020, the HKMA issued a circular identifying examples of good practices following its thematic review of AML control measures for remote customer onboarding. It is essential for banks which rely on "off-the-shelf" solutions to demonstrate an appropriate level of understanding of how the solutions work, both in terms of their benefits and limitations such as the features or attributes matched by artificial intelligence in the identity authentication process and algorithms used. With appropriate understanding, this will simplify the implementation process, reduce the risk of the technology solution delivering unintended outcomes and lead to more effective management of

Jurisdiction	
	AML risks. Other good practices include due diligence of the vendor's capability and reliability, and ongoing quality assurance processes on the technology deployed, such as 100% manual checking of 'selfie' images and identity documents. In terms of government initiatives to facilitate the remote onboarding of customers through technology, the Office of the Government Chief Information Officer launched iAM Smart in December 2020. In a circular on the same date, the HKMA encouraged banks to actively consider adopting iAM Smart. This provides all Hong Kong residents with a single digital identity and means of authentication through biometrics in their personal mobile devices which will have been verified against their Hong Kong Identity Cards during the iAM Smart registration process. The HKMA AML FAQs and a May 2021 circular state that iAM Smart can satisfy customer identification and verification requirements under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO), including associated record-keeping requirements through retaining data obtained from iAM Smart by way of an Application Programming Interface (API). **Tech adoption in transaction monitoring** In a public speech in September 2018, the deputy chief executive of the HKMA endorsed banks' use of machine learning and artificial intelligence to help detect and recognise suspicious behaviours and patterns, as well as to facilitate the closing of low-risk alerts. In the June 2020 edition of Regtech Watch, the HKMA highlighted regtech use cases in transaction monitoring and suspicious activity reporting, including the use of supervised machine learning to tackle the problem of high false positives and the application of advanced data mining techniques to expanded data pools to trace and identify networks of transactions and counterparties associated with customers. The HKMA has further provided guidance whereby a bank should be conversant with the abilities of the algorithm used in its transaction screening system, with particular attention being paid to the ability of the name screening system to identify names with minor alterations, such as names in reverse order, partial names and abbreviated names. In the HKMA's press release in November 2021 announcing disciplinary actions against four banks for AMLO contraventions, it set out its expectations going forward, including referencing the case examples to review data quality and transaction monitoring system effectiveness, and that the risk-based approach in banks' AML efforts be premised on an up-to-date understanding of evolving risks and responsible innovation, including regtech adoption. For more, see our briefing **HKMA Penalises Four Banks HK$44 Million For Money Laundering Control Failures: Key Takeaways**. **HKMA support to industry for tech adoption** In a circular in August 2021, the HKMA highlighted the Financial Action Task Force (FATF) July 2021 report, which discusses how new technologies such as machine learning and natural language processing can improve the speed, quality and effectiveness of AML measures. In line with global efforts, the HKMA has been taking steps to support AML innovation and strengthen banks' adoption of new technologies by identifying the common operational challenges encountered and carrying out activities to assist with overcoming these challenges. This began with industry engagement by way of the AML Regtech Forum in November 2019. Throughout 2020, conversations took place with approximately 40 banks to better understand how regtech was being approached to enhance AML processes; this culminated in the publication of a report in January 2021 sharing the banks' experiences. The report provides technology spotlights and guidance on addressing challenges such as data and process readiness, executive support and stakeholder buy-in, as well as working with third-party vendors. In July 2021, a Regtech Adoption Practice Guide was issued to help banks assess whether they have appropriate governance, controls, skills, infrastructure and underlying data to enable them to apply regtech solutions that assist AML efforts in the area of ongoing monitoring of customers. This has been accompanied by activities such as interactive lab sessions using synthetic data.

Jurisdiction	
China	The PRC Anti-Money Laundering Law (the PRC AML Law) issued by the Standing Committee of the National People's Congress does not specify the use of any particular technologies for the purpose of AML compliance functions. The People's Bank of China (PBoC), which is the primary regulator in charge of monitoring AML compliance across financial industries, has issued some high- level regulations and guidance suggesting that regulated entities adopt certain technical measures to perform AML obligations. For example, regulated entities (including financial institutions and certain non-financial institutions) are required to (i) take technical security measures to strengthen internal management procedures and to verify client identities, and (ii) ensure that the necessary technologies have been adopted for money laundering risk management and proper information systems have been employed to improve efficacy and efficiency. For banking financial institutions, the Administrative Measures for Anti-money Laundering and Counter-terrorism Financing for Banking Financial Institutions issued by the China Banking and Insurance Regulatory Commission (CBIRC), the primary regulator for the banking and insurance industry, additionally specify that banking financial institutions should employ and embed quantifiable anti-money laundering indicators into the relevant information system for early warning, effective transmission and sharing of risk information, information extraction, analysis and reporting of money laundering risks. In addition, prior to applying a new technology, a financial institution shall conduct risk assessments for money laundering and terrorism financing. Note that the Guidelines for the Management of Money Laundering and Terrorist Financing Risks of Incorporated Financial Institutions (Trial Implementation) issued by PBoC in September 2018, which became effective as of 1 January 2019, sets forth detailed requirements in this regard. However, no use of any specific technology or method has been prescribed.
Singapore	The Monetary Authority of Singapore (MAS) does not mandate the use of specific technologies. The MAS has issued guidelines on Singapore client authentication, but those guidelines do not prescribe the use of any specific technology or method. These guidelines are not legally binding, although the degree of observance with the spirit of the guidelines is an area of consideration in the risk assessment of the financial institution by MAS. On 4 November 2021, the Deputy Chief FinTech Officer of MAS clarified that MAS is a strong advocate when it comes to the use of technology in financial firms. Such technology, or regtech, seeks to support FIs based in Singapore to enhance their risk management and compliance functions using technological solutions. In April 2021, MAS launched a regtech grant of S$12 million to support FIs to develop capabilities towards risk management or regulatory compliance. In the first six months of the grant, MAS allocated close to 10% of the amount to relevant regtech projects. These grants may be used to support commercial off-the-shelf regtech solutions or even prototype regtech solutions.

Jurisdiction	
Japan	Certain forms of electronic signature authorisation are permitted as one of the customer identification verification methods required in the 'know your customer' checks under the Act on the Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007, as amended) (the PTCP Act). The PTCP Act is the principal act concerning AML in Japan and requires certain business operators, including financial institutions, credit card companies, cryptocurrency business operators, real estate agents and precious metal/stone dealers, to conduct customer verification when they enter into certain restricted transactions with new customers. Customer verification must be conducted by one of the designated methods under the PTCP Act. One such designated method, permitted if the relevant party is an individual, is by sending an email with an electronic certificate issued in accordance with the Electronic Signatures and Certification Business Act (Act No. 102 of 2000, as amended) (the ESA Act). An electronic certificate must include the name, address and date of birth of the relevant individual and must be issued by a designated authorisation agency. Such designated authorisation agencies are licensed private companies. Alternatively, an electronic certificate issued pursuant to the Act on Certification Business of Local Governments in Relation to Electronic Signatures (Act No. 153 of 2002, as amended) is accepted instead of the electronic certificate issued under the ESA Act. Such electronic certificates are issued at a local government level and are stored electronically in Japanese residents' Individual Number Cards (public ID cards). In relation to an entity, an electronic certificate will only be accepted if the electronic certificate is issued by an officer of the company's public registration system pursuant to the Commercial Registration Act (Act No. 125 of 1963, as amended). The Payment Services Act (Act No. 59 of 2009, as amended) was amended in June 2022 (to come into force no later than June 2023) and following the amendments, issuers of e-money who transfer amounts of high value (i.e., exceeding ¥0.1 million in one transfer or a total of transferred amounts in one month exceeding ¥0.3 million) will be required to carry out KYC checks in accordance with the PTCP Act.
Australia	There are no requirements for specific technologies to be used in performing AML compliance functions. Australia's AML regulator, the Australian Transaction Reports and Analysis Centre Australia (AUSTRAC) provides that there is no 'one-size-fits-all' technology or AML programme for reporting entities. Entities should develop and utilise tailored technologies to meet their specific needs, risk and characteristics to develop stronger AML/CTF controls. Reports to AUSTRAC can most easily be made through the AUSTRAC online portal, in which reporting entities must enrol and they must register with AUSTRAC within 28 days of providing a designated service. Some additional programs may assist, such as the use of online data entry, spreadsheets or extraction for larger businesses. If an entity wants to make use of the XML extraction method of reporting, it must undergo an "XML test file process" to ensure that the extraction program meets the XML file format schema and specifications.

7.2 Are regulated entities in your jurisdiction allowed and/or encouraged by regulators to use commercially available 'know your customer' registries, name screening services, or other shared utilities to carry out AML-related functions?

Jurisdiction	
Hong Kong	Hong Kong regulators recognise and allow the use of such services. The AML guidelines published by the SFC and the HKMA allow flexibility in the measures permitted for verifying a customer's identity so as to acknowledge technological developments in the methods used by financial institutions. Both the SFC and the HKMA have endorsed the use of commercially available databases for screening whether customers, their beneficial owners and connected parties are politically exposed persons, the source of wealth and funds of high-risk customers, and sophisticated name screening systems against terrorist/sanction designations as examples of good or reasonable AML practices adopted by licensed corporations. They have, however, declined to prescribe specific examples of comprehensive and reliable databases or registries. They have also stressed that when using commercially available databases, a licensed corporation should be aware of their fitness for purpose and limitations, depending on the source of the underlying data, including whether it only encompasses publicly available information, the definition of politically exposed person used and any deficiency in technical capability. Appropriate measures should be taken to ensure the completeness and accuracy of commercial databases of terrorists and designated parties; for example, by conducting periodic sample testing.
China	Under the current PRC AML regime, regulated entities are still obliged to collect and verify identity information provided by customers, instead of exclusively relying on recorded information from registries, services or other utilities. However, a range of documentation and electronic data available on the relevant facilities run by the government may be used to verify such information. In January 2019, the government launched an online monitoring platform for anti-money laundering in the internet finance industry for trial operation, which will be used to improve the online regulatory mechanism for anti-money laundering and strengthen information sharing. In addition, the PRC government generally encourages regulated entities to use new technologies, including big data and cloud computing, to promote efficiency in the AML process and the government plans a further rollout of its governmental information- sharing system.

Jurisdiction	
Singapore	Singapore regulators generally encourage the use of such registries, services or utilities subject to the usual risk management issues. In our experience, most local financial institutions use screening software provided by reputable third parties. In July 2017, the MAS worked with the private sector to explore the establishment of a joint KYC utility. However, the project was put on hold in September 2018 as a result of cost concerns. This has shown that data standardisation required by a centralised KYC registry may be costly. For example, institutions had to make significant investments to migrate historical bank data to the utility and to integrate individual banks into the system. Nevertheless, Singapore has successfully implemented an e-KYC programme that enables Singaporean customers to use their MyInfo profile via the Singpass application to open accounts. MyInfo contains data provided by the user and data pulled from databases of various government agencies such as national ID number, passport number, registered address, and date/country of birth. Once consent has been given, a financial service provider need not obtain further identity verification or a photograph of the customer. This proved useful during the COVID-19 pandemic, where FIs could continue onboarding new clients remotely. For businesses, MyInfo Business allows them to share their government-verified data, such as corporate profile, financial performance, and ownership information through the platform with financial service providers. This reduces overheads by reducing form-filling and the need to provide supporting documentation for verification.
Japan	In Japan, exclusion of Anti-Social Forces (ASFs) initiatives is widely conducted in financial institutions and various other industries. ASFs are defined as the Japanese yakuza (mafia) and other anti-social bodies and their members. Accordingly, business operators are strongly encouraged to conduct ASF checks within their 'know your customer' process and to include a provision in relevant contracts to terminate the transaction immediately if it is found that the counterparty is an ASF. ASFs are categorised as a high-risk group from an AML perspective and accordingly such ASF checks would be an integral part of the AML safeguards. To conduct an ASF check, there are no official databases of ASF parties that are open to the public. Members of the Japanese Bankers Association (JBA) can access the ASF database maintained by the National Police Agency of Japan through the Deposit Insurance Corporation of Japan, in cases where the KYC check is carried out for advances of personal loans given by member banks of the JBA. ASF screening is sometimes conducted through such databases. The amended Payment Services Act will introduce new licensing requirements for certain operators performing transaction monitoring on an outsourced / large scale basis in order for financial institutions to facilitate and encourage the use of such operators in conducting joint AML operations as well as ensuring the quality of provision of such service through supervision by regulators.

Jurisdiction	
Australia	Amendments to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)* (AML/CTF Act) came into effect on 18 June 2021. These allow reporting entities to rely on customer identification procedures and information, also known as 'know your customer' (KYC) procedures, provided by a reliable third party. Third-party customer identification procedures may be relied upon by reporting entities in two circumstances. Sections 37A and 37B of the AML/CTF Act allow reporting entities to rely on customer identification procedures conducted by third parties if: a) a written agreement or arrangement (known as a Customer Due Diligence (CDD) arrangement) has been entered into with the third party; b) the reporting entity has reasonable grounds to believe that the reliable third party is complying with the KYC requirements in the AML/CTF rules; and c) the reporting entity carries out regular assessments of the third party's performance and compliance with the AML/CTF rules and prepares a written record of each assessment within 10 business days. Section 38 of the AML/CTF Act is a broader provision which allows reporting entities to rely on customer identification procedures conducted by third parties on a case-by-case basis even without a CDD arrangement in place. Reporting entities may rely on this provision if they believe that the third party has complied with the requirements prescribed by the AML/CTF rules and it would be appropriate to rely on the third party's identification procedures, taking into account the ML/TF risks and matters under the AML/CTF rules. Otherwise, there is no official encouragement to use any specific registers or services, although there have been unsuccessful attempts to amend Australia's AML frameworks to allow entities to rely on information recorded in relevant registries, rather than being required to collect information from the customer. Entities are still required to collect the relevant information from the customer; however, a range of documentation and electronic data can be used to verify that information. AUSTRAC has noted that one option for verifying individual customer and beneficial owner identification using electronic data is the Document Verification Service (DVS), a secure online system managed by the Department of Home Affairs. The DVS matches government-issued identity documents directly with the government organisation that issued them, which also enables organisations to monitor in real time if the document is current or has been reported lost or stolen. AUSTRAC also issued guidance in the context of the COVID-19 pandemic, providing guidance on the completion of KYC and verification checks in circumstances where in-person meetings are not possible.

7.3 Are there consumer data protection or other restrictions that may prevent entities in your jurisdiction from offshoring AML compliance functions?

Jurisdiction	
Hong Kong	Personal data is protected by the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). There is no restriction on the transfer of personal data outside Hong Kong as there is currently no set timeline to bring section 33 of PDPO addressing this issue into force. However, to comply with Data Protection Principle 1 of the PDPO, the information collector must spell out clearly in the personal information collection statement that the personal information collected will be transferred to, or used by, offshore AML compliance functions. The offshore functions also need to comply with other requirements in the PDPO, any extraterritorial restriction imposed by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) and, in certain jurisdictions, local data protection laws and regulations. Paragraphs 4.15 and 4.11 of the respective AML guidelines issued by the SFC and HKMA also contain guidance for financial institutions which rely on intermediaries for customer due diligence.
China	Client data is protected by various laws and rules in China, including the PRC AML Law. The PRC AML Law generally requires that regulated entities should take necessary management and technology measures to prevent the loss, destruction or disclosure of clients' identity information or transaction data. In addition, the Regulations on Financial Institutions' Anti-money Laundering issued in 2003 and amended in 2006, and the Administrative Measures for Anti-money Laundering and Counter-terrorism Financing for Banking Financial Institutions issued in 2019, require financial institutions to keep the following information confidential: (i) client identification data and transaction data acquired in the process of performing anti-money laundering duties; and (ii) any information related to anti-money laundering (e.g., the reporting of suspicious transactions and assistance in the investigation of doubtful transactions). Unless permitted by PRC law, the client identification information and transaction information acquired during these checks may not be provided to any individuals or legal entity (including offshore individuals or entities), even if consent of the relevant clients is obtained. Accordingly, given that no law or administrative regulation has provided for an explicit exception for the cross-border transfer of the AML Information, offshoring AML compliance functions is not permitted under the current regulatory regime.
Singapore	Personal data is protected by the Personal Data Protection Act 2012 (PDPA). Under the PDPA, an organisation is not permitted to transfer any personal data outside Singapore except in accordance with requirements prescribed to ensure that organisations maintain a comparable standard of protection for personal data to that under the PDPA. This could be done, for example, by having a contract that requires the recipient to maintain such standards and which specifies the countries and territories to which the personal data may be transferred. Financial institutions have to ensure that the transfer of such data complies with banking secrecy requirements. In addition, they may wish to observe MAS Guidelines on Outsourcing (issued in 27 July 2016, last revised on 5 October 2018), which contain prudent practices on risk management of outsourcing.

Jurisdiction	
	For restrictions specific to offshoring AML compliance functions, the guideline states that institutions wishing to engage an overseas service provider should conduct proper due diligence of the service provider's external environment, such as the political, economic, social, and legal environment of the jurisdiction it operates in. Such due diligence includes: • the service provider's ability to comply with applicable laws and regulations; the service provider's regulatory compliance track record is also reviewed; • a foreign government's policies; • the institution's ability to effectively monitor the service provider, and its ability to execute its business continuity management plans and exit strategy; • disaster recovery arrangements; and • other locations established by the service provider in relation to the outsourcing arrangement. For instance, information and data could be moved to primary/back-up sites located in other foreign countries. The institution should consider the risks associated with the medium of transport (physical or electronic). Additionally, outsourcing arrangements should: • be tailored to address issues arising from country risks, i.e., economic, social and political conditions and events in a foreign country that may adversely affect the institution; • include a choice of law provision; • be entered into only with foreign service providers operating in jurisdictions that uphold confidentiality clauses and agreements; • not be entered into with foreign service providers in jurisdictions where prompt access to information by MAS may be impeded by legal or administrative restrictions: – an institution must commit to retrieve information from the service providers upon MAS' request. – the institution should confirm in writing to MAS that it has provided in its outsourcing agreement for MAS to have the rights of inspecting the service provider and rights of access to the institution's and service provider's information, reports and findings related to the outsourcing agreement. – provide for the institution to notify MAS if any overseas authority were to seek access to its customer information or if rights of access of the institution and MAS have been restricted or denied.

Jurisdiction	
Japan	Personal data is protected by the Act on the Protection of Personal Information (APPI). The APPI was amended in 2017 and, thereby, transfer of personal data to an overseas third party, including a data processor, may not, in principle, be made without the relevant data subject's specific consent. Further amendments were implemented in 2022, introducing the obligation to provide necessary information to the data subject prior to giving such consent, including, but not limited to, information regarding the country to which the data will be transferred, the system for protection of personal information in such country, measures to be applied by the third party who receives such data to such cross-border data transfer unless any of the exemptions (e.g., in case such transfer is required by Japanese law) applies or any of the following conditions are met: (i) the third party is located in the country which is recognised by the Personal Information Protection Commission (PPC) as having a personal information protection system conforming to the standards required by the APPI to protect individuals' rights and interests (the PPC currently recognises only member countries of the European Economic Area and the UK); or (ii) the overseas third party has established a system conforming to standards prescribed by the PPC rules as necessary to enable the taking of actions equivalent to those that a Japanese operator must take in accordance with the APPI. If either of the above conditions is met, personal data may be transferred to an overseas third party as if the third party is located in Japan. Domestic transfers of personal data may be made based on the consent of the relevant data subject or by taking specific measures to transfer personal data without consent. In the case of (ii) above, the following measures must be taken after the transfer of personal data to an overseas third party, in order to ensure continuous data protection measures (to the level required by the APPI) are implemented by such third party: (a) regular checks on the measures implemented by the third party who receives the data, and the presence and the content of the data protection system established in such country, which may influence the appropriateness and reasonableness of the method of data protection implemented; and (b) taking necessary and appropriate measures when the third party encounters a problem in implementing such measures, and stopping the transfer of personal data to such third party when it is difficult to ensure continuous data protection measures to the level required by the APPI. If a business operator's acts are in breach of the regulations above, the PIPC can advise the operator to take necessary measures to protect personal rights and interests, including the cancellation of such acts to cure the breach. In the case of financial institutions, confidentiality and bank secrecy would raise a need to consider whether offshoring/outsourcing AML compliance functions is allowed, as well as considering the requirements under the APPI above.
Australia	Section 37 of the AML/CTF Act allows for customer identification and verification procedures to be carried out by agents of a reporting entity. The reporting entity remains liable for its 'know your customer' obligations, regardless of the fault of the agent. The Act does not specify whether these agents need to be located within Australia. The Australian Privacy Principles (APPs) regulate the cross-border disclosure of personal information, particularly APP 8, which may be relevant in considering the offshoring of AML compliance functions. APP 8 states that entities subject to the APPs must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the APPs. However, APP 8 does not apply to the transfer of personal data where the overseas recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to how the APPs protect the information, and mechanisms can be accessed by the individual to enforce that protection of the law or binding scheme.

7.4 What are the types of technology deficiencies that are most likely to result in AML-related regulatory findings in your jurisdiction? Are there any well-known examples of enforcement cases?

Jurisdiction	
Hong Kong	The lack of an adequate system to monitor, identify and follow up with Politically Exposed Persons (PEPs) is likely to lead to adverse regulatory findings. In April 2017, a private bank and wealth manager was fined HK$7 million by the HKMA for contravening the AMLO. One of the contraventions was that the bank did not check or monitor whether its existing customers had become PEPs. In addition, although the bank received alerts from commercially available databases that its existing customers had become PEPs, it lacked a management reporting system to ensure that such alerts were followed up by senior management in a timely manner. Similarly, another bank had earlier been fined HK$7.5 million by the HKMA. One of its contraventions was the lack of periodic review of whether existing customers were PEPs. In February 2020, a securities firm was fined HK$3.7 million by the SFC and again, one failure was it not putting in place adequate and effective procedures for the identification of PEPs.
China	Regulated entities are required to: (i) take technical security measures to strengthen internal management procedures and to verify client identities; (ii) ensure that the necessary technologies have been adopted for money laundering risk management; (iii) establish and implement a complete client identity data and transaction record-keeping storage system; and (iv) establish that proper information systems have been employed and quantifiable anti-money laundering indicators embedded into the relevant information system for early warning, effective transmission and sharing of risk information, information extraction, analysis and reporting of money laundering risks. Regulated entities and their directors and managers directly responsible are jointly liable if they fail to perform duties to identify and keep records of clients' identities and transactions, to report suspicious transactions, etc. We are not aware of any previous occasions where technology deficiencies have clearly led to an AML-related regulatory finding.
Singapore	There has not been any reported case in Singapore where a technology deficiency has clearly led to an AML-related regulatory finding. The investigation and enforcement action related to the 1Malaysia Development Berhad (1MDB) fund flows through Singapore is one of the most prominent local AML enforcement cases and, while it involved PEP issues, it is not clear from publicly available materials that it stemmed from technology deficiencies.
Japan	For the purpose of compliance with the Act on the Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007, as amended) (the PTCP Act), technology deemed appropriate according to relevant regulations should be used to confirm customers' and other parties' identification and information. Even if a technology is commonly used in other jurisdictions for the purpose of KYC, use of such technology may be deemed inappropriate under the PTCP Act, and a breach of the PTCP Act. Having said that, the minimum acceptable due diligence procedures and expectations may also change from time to time, recognising that information resources change and undergo innovation across markets. In addition, regulated entities should take into account requirements and supervisory points in respect of AML compliance under specific regulations and guidelines concerning its regulated business. Consequently, in order to avoid criticism or sanction, it is important to keep abreast of such changes and to regularly review and update due diligence procedures.

Jurisdiction	
Australia	AUSTRAC is arguably Australia's most feared corporate regulator, following a series of high-profile successful prosecutions of major Australian corporations. Its most significant regulatory findings have resulted from failures by large organisations to adequately monitor patterns of activity in their network. In March 2017, Tabcorp, an Australian gambling and entertainment company, settled with AUSTRAC and paid an AU$45 million civil penalty, plus legal costs, for breaches of AML and counter-terrorist financing (CTF) contraventions. The Court found that Tabcorp had failed to have a compliant AML/CTF programme, failed to give AUSTRAC reports about suspicious matters on time, or at all, on 105 occasions, and failed to identify a customer who had won AU$100,000 and failed to enrol with AUSTRAC on time. As part of the settlement agreement, Tabcorp introduced automatic transaction monitoring capabilities. In June 2018, AUSTRAC and the Commonwealth Bank of Australia (CBA) reached an AU$700 million settlement of enforcement proceedings commenced by AUSTRAC alleging "serious and systemic non-compliance" with the AML/CTF Act. AUSTRAC's enforcement action against CBA followed exhaustive investigations into CBA's AML/CTF compliance and risk management practices, particularly in relation to its Intelligent Deposit Machines (IDMs), which were being used to launder proceeds of crime. CBA admitted various contraventions of the AML/CTF Act, including that: • it failed to carry out an appropriate assessment of the money laundering and terrorism financing (ML/TF) risks of its IDMs prior to October 2017; • it failed to complete the introduction of appropriate controls to mitigate and manage the ML/TF risks of IDMs prior to April 2018; • it failed to provide on time 53,506 threshold transaction reports to AUSTRAC for cash transactions of AU$10,000 or more through IDMs from November 2012 to September 2015, having a total value of approximately AU$625 million; and • for a period of three years, it did not comply with the requirements of its AML/CTF programme relating to monitoring transactions on 778,370 accounts. In October 2020, the Federal Court of Australia approved a record AU$1.3 billion fine imposed on Westpac Banking Corporation (Westpac) for breaching the AML/CTF Act on 23 million occasions. Westpac admitted that it had failed to report over 19.5 million international funds transfers into and out of Australia, some of which involved transactions in high-risk jurisdictions. Westpac also admitted a failure to keep proper records and conduct adequate due diligence on customer accounts. The Federal Court's approval of AUSTRAC's AU$1.3 billion penalty on Westpac represents the highest corporate penalty issued in Australia. AUSTRAC has also issued guidance to assist organisations with managing risks arising from particular technologies. In April 2022, AUSTRAC issued guidance on detecting and reporting ransomware payments related to financial crime, and a guide to assist financial service providers, including digital currency exchange providers, to identify and report criminal activity facilitated through digital currencies. In November 2021, AUSTRAC also issued guidance to help businesses understand, identify and report technology facilitated abuse through financial transaction payment text fields.

7.5 Have any regulators in your jurisdiction issued AML-specific guidance and/or regulations concerning new or emerging technologies such as mobile payments, digital currencies, blockchain, artificial intelligence or others?

Jurisdiction	
Hong Kong	**Electronic payments** Electronic payment services operated by banks, deposit-taking companies, retail payment system operators (for example, Visa, Mastercard, UnionPay, JETCO and EPS) and stored-value facility (SVF) operators (such as Octopus, Alipay, WeChat Pay, Autotoll and PayPal) are required to be licensed or designated by the HKMA and subject to one or both of the Banking Ordinance (Cap. 155) and Payment Systems and Stored Value Facilities Ordinance (Cap. 584). In terms of AML regulation or guidance, SVF licensees are subject to the AMLO, including requirements in Schedule 2 to the AMLO such as those relating to customer due diligence, ongoing monitoring of customers, suspicious transactions reporting and record-keeping. The HKMA has also issued a specific Guideline on AML and Counter-Terrorist Financing (CTF) (For SVF Licensees) in September 2016, which was revised in September 2020. The guideline applies to all SVF licensees for the issue of an SVF. **Virtual currencies** Apart from the above, the HKMA and SFC have issued circulars to remind financial institutions of various risks associated with virtual currencies such as Bitcoin. On 5 September 2017, the SFC issued a statement on existing regulations which could be applicable to initial coin offerings (ICOs). In the statement, the SFC observed that ICOs may be classified as "securities" and hence within the ambit of Hong Kong securities laws. This was followed up by a number of statements in February and March 2018 and March 2019 in which the SFC reported its action in warning or halting certain ICOs, and reminded the public of the risks in ICOs or security token offerings (STOs). In November 2018, the SFC issued guidance on the regulatory standards expected of virtual asset portfolio managers and fund distributors, and on a conceptual framework for virtual asset trading platform operations (or cryptocurrency exchanges). In November 2019, in relation to virtual asset trading platform operations, the SFC clarified the conceptual framework and provided for an opt-in regime. The Financial Services and the Treasury Bureau (FSTB) has since carried out a consultation on legislative proposals to enhance the AML and CTF regime and introduce a licensing regime for persons operating a virtual asset exchange in Hong Kong as licensed virtual asset service providers (VASPs) under the AMLO. Consultation conclusions were published in May 2021. The relevant amendment bill has been introduced in the Legislative Council for its first reading in July 2022 and is expected to be passed before the end of 2022. The new regime is proposed to take effect on 1 March 2023. Licensed VASPs will be subject to requirements in Schedule 2 to the AMLO. The SFC will be empowered to impose licensing conditions, as well as regulatory requirements. See **section 11** on Fintech. **AI** There is no specific legislation regulating artificial intelligence (AI) in Hong Kong. The government, however, has banned certain AI products, specifically autonomous vehicles that do not require a human driver.

Jurisdiction	
	There is growing use of AI in the financial sector. The stance of both the SFC and HKMA on the use of technology, including AI, is based on the principles of technology neutrality and risk-based supervision. The SFC has not issued any AI-specific guidance, although it did issue the Guidelines on Online Distribution and Advisory Platforms in June 2019 in which there is a specific chapter on robo-advice (provision of financial advice in an online environment using algorithms and other technology tools). The HKMA, on the other hand, has developed supervisory guidelines for banks to follow when applying AI with the aim of strengthening corporate governance in three key areas – AI model risk management, cybersecurity and consumer protection. That said, the guidelines do not concern AML. Also, albeit unrelated to AML, the Privacy Commissioner for Personal Data issued Guidance on Ethical Development and Use of AI in August_2021 to help organisations understand and comply with the relevant requirements of the Personal Data (Privacy) Ordinance when they develop or use AI.
China	PBoC, CBIRC and the China Securities Regulatory Commission (the primary regulator for the securities industry, CSRC) issued the Administrative Measures for Anti-money Laundering and Counter-terrorism Financing by Internet Finance Institutions (Trial Implementation) (Administrative Measures for Internet Finance Institutions) to regulate anti-money laundering matters in the internet finance industry, including, but not limited to, online payment, internet fund sale, internet consumer finance and peer-to-peer lending. The requirements set out in the Administrative Measures for Internet Finance Institutions are substantially the same as those for other financial institutions. On 4 September 2017, a cross-agency working committee in China (led by the PBoC, and including the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology, the State Administration of Industry and Commerce, the CSRC, the China Banking Regulatory Commission and the China Insurance Regulatory Commission (which were integrated and now known as CBIRC)) issued the Circular on Preventing Risks related to Initial Coin Offerings (Circular). According to the Circular, ICOs are described as an unauthorised and illegal public fundraising activity in nature, and may constitute a number of crimes such as illegal quasi-currency instruments offerings, illegal securities offerings, illegal fundraising, financial fraud and pyramid selling schemes. The Circular ordered an immediate halt to all ICOs in China and financial institutions and non-banking payment institutions were prohibited from directly or indirectly providing any ICO-related services (such as account opening, registration, trading, settlement, clearing and ICO-related insurance). This position has been affirmed by various circulars issued by regulators subsequent to the Circular. In 2019, the CAC issued the Administrative Measures on the Blockchain Information Services (Blockchain Measures), which became effective as of 15 February 2019, to govern the provision of blockchain information services within the territory of China. According to the Blockchain Measures, blockchain information service providers must make the required filing with the online system operated by the CAC within 10 business days following the provision of blockchain information services and must implement relevant internal management mechanisms as required under the Blockchain Measures. The authorities have also taken action to counter money laundering in connection with emerging technologies. According to the Notice on Further Preventing and Dealing with Speculation Risks in Virtual Currency Trading issued in 2021, the authorities have been conducting special campaigns to crack down on money laundering and gambling through virtual currencies. Typical AML cases published by the Supreme People's Procuratorate in 2021 include a case where the accused was criminally penalised for committing money laundering through virtual currencies.

Jurisdiction	
Singapore	MAS clarified on 5 April 2021 that it has taken three steps to address AML/CFT risks associated with cryptocurrencies. First, digital payment token service providers – entities involved in providing cryptocurrency-related services – need to be licenced by MAS. Existing virtual asset service providers operating in Singapore were required to notify MAS and submit licence applications by 28 July 2020. The applicants were expected to demonstrate an ability to mitigate ML risks. As of 28 January 2020, such entities are subject to the Payment Services Act in Singapore. They must comply with AML/CFT requirements such as obligations to perform customer due diligence and transaction monitoring. They are also required to file suspicious transaction reports with the Commercial Affairs Department (CAD). MAS takes a risk-sensitive approach where activities that pose higher ML risks (e.g., cross-border peer-to-peer money transfers) are subject to the full suite of requirements. On the other hand, low-risk ML activities (e.g., payment for goods/services funded through an account maintained with an MAS-regulated FI subject to AML requirements) will not be subject to AML requirements. Further amendments were made to the Payment Services Act in January 2021 to include additional digital payment token activities such as providing custodial wallet services and facilitating the transfer of digital payment tokens. Secondly, MAS has stepped up surveillance of the cryptocurrency sector to identify suspicious networks and higher risk activities for further supervisory scrutiny. MAS' surveillance efforts are focused on (a) detecting and deterring unlicensed digital payment token activities in Singapore and (b) leveraging data and blockchain analytics to identify higher risk entities. Thirdly, MAS and the CAD continue to raise public awareness on the risks of investing in digital payment tokens through MAS' advisories and public education efforts. These advisories will provide consumers with information on how to avoid being cheated or inadvertently used as money mules to carry out ML activities. As the cryptoassets realm is constantly evolving, MAS closely monitors developments and will continue to adapt its rules as required to ensure that regulation remains effective and commensurate with the risks posed. In the meantime, MAS encourages investors to exercise extreme caution when trading cryptocurrencies. Looking into the future, MAS seeks to launch COSMIC in 2023, a platform for FIs to collaborate using data analytics to combat the risks of money laundering. In its initial phase, COSMIC will focus on risks related to the abuse of shell companies, illicit misuse of trade finance, and evasion of United Nations sanctions.
Japan	The amendments to the Banking Act (Act No. 59 of 1981, as amended), which became effective as of 1 April 2017, require Cryptoassets Exchange Service Providers (CAE) (formerly known as Virtual Currencies Exchange Service Providers) to be licensed. At the same time, CAEs have been added as a designated business operator and are therefore obliged to comply with AML requirements under the Act on the Prevention of Transfer of Criminal Proceeds (Act No. 22 of 2007, as amended) (PTCP Act). The amended Payment Services Act (Act No. 59 of 2009) (the amendments will come into force by no later than June 2023) has become the first legislation in the world to regulate stablecoins. The new framework under the amendment covers asset-linked currency-based stablecoins as "electronic payment instruments". Intermediaries of "electronic payment instruments" will be subject to a new licensing requirement for performing intermediary functions such as the transfer and management of stablecoins. A firm obtaining the new licence will also be subject to codes of conduct, such as anti-money laundering and countering the financing of terrorism.

Jurisdiction	
Australia	Since 2018, the AML/CTF Act has applied to convertible digital currencies, through regulation of digital currency exchanges. AUSTRAC has published guidance to assist digital currency exchange businesses to register with AUSTRAC and comply with its ongoing requirements. As mentioned above, in April 2022, AUSTRAC released guidance on criminal abuse of digital currencies to help financial service providers identify and report criminal activity facilitated through digital currencies. More generally, the Australian Securities and Investment Commission (ASIC) has been a leading force in fintech and regtech developments in the region. It has provided a safe space – a regulatory sandbox – which allows eligible start-up companies to test their products subject to certain conditions whilst being exempt from usual licensing requirements for a prescribed period. ASIC also released a consultation paper in March 2022 on a proposed regulatory model to administer a licensing framework and establish crypto custody requirements for cryptoasset second service providers (CASSPRs), who provide services to retail and business customers to facilitate access to and use of cryptoassets such as custody, storage, exchange, brokerage, and operating a crypto market. In an AML/CTF context, the licensing regime for CASSPRs aims to support the current AML/CTF regime administered by AUSTRAC and protect consumers from any harm that may arise from criminals and their associates owning or controlling CASSPRs. In October 2021, ASIC issued updated regulatory guidance (Information Sheet 225) to help businesses understand their obligations under the Corporations Act 2001 (Cth), the Australian Securities and Investment Commission Act 2001 (Cth) and other Australian laws in connection with cryptoassets and initial coin offerings. The information sheet provides guidance in relation to: • considerations when offering cryptoassets through an ICO; • misleading or deceptive conduct in relation to an ICO or a cryptoasset; • when an ICO might be or involve a financial product; • when a cryptoasset trading platform could become a financial market; • financial products that reference cryptoassets; and • the translation of overseas categorisations of cryptoassets into the Australian context.

SANCTIONS AND EXPORT CONTROL

8. SANCTIONS AND EXPORT CONTROL

China and the US

Former President Trump rolled out a wide range of restrictive measures against China during his term in office between 2017 and 2020, which were implemented with bipartisan support. The Trump Administration's introduced new sanctions on entities from the Xinjiang region, restrictions on US investment into certain Chinese military entities, required the divestment of subject securities, and heightened the scrutiny of Chinese investment into the United States via the CFIUS process. Key aspects of the Trump administration's sanctions and export controls against China have survived or even augmented, while fresh eyes and scrutiny based on a targeted and precise approach have led to adjustments to the controversial or legally vulnerable measures.

In June 2021, President Biden **revoked** an executive order that would have restricted the use of eight popular Chinese apps, including TikTok and WeChat, in the United States. In its place, the Commerce Department was instructed to conduct an evidence-based evaluation and take appropriate action against connected software applications. Further guidance is expected.

In February 2022, the Department of Justice **announced** that its China Initiative, with the apparent aim of thwarting economic espionage and trade secret theft, was not the right approach.

Export control

On the export control side, the Trump Administration revamped and expanded the military end use rule, preventing exports of certain items intended for military end use to China. As well as a military end user list, there is also an Unverified List (UVL) which refers to the inability to verify end use, and US exporters seeking to export to entities on such list must obtain a licence to do so. Entities on the UVL are mostly high-tech manufacturers including those producing laser components, government research laboratories and universities. In February 2022, the US Commerce Department's Bureau of Industry and Security **added** 33 Chinese companies to the UVL. The Entity List is another list of entities subject to export control and Chinese technology companies including **biotechnology, chip and semiconductor**; **quantum computing** and **supercomputing** companies have been added under President Biden.

Xinjiang import restrictions

In December 2021, the United States passed **legislation** imposing a rebuttable presumption standard for prohibiting the import of goods made in Xinjiang in response to perceived activity there. The implementation of this legislation commenced on 21 June 2022. Although not a traditional "sanctions" measure, the US Customs and Border Protection previously had the power to and did actively issue Withhold Release Orders (WROs) on certain products and entities originating in the Xinjiang region, which effectively served as seizure notices for such goods upon import into the United States. This power has been broadened under the new legislation.

So-called 'Chinese Military-Industrial Complex Companies' security purchase restrictions

Former President Trump's actions against China also included prohibiting US persons from engaging in transactions for the purchase of publicly traded securities of or derivative of so-called Communist Chinese Military Companies (CCMC). In June 2021, President Biden revamped and expanded these restrictions, creating a **new securities-related sanctions regime** in relation to so-called 'Chinese Military-Industrial Complex Companies' (CMIC). The new measures expand the criteria for designation beyond Chinese military companies to include companies in the surveillance technology sector of China's economy and add new entities to the subject restrictions. In December 2021, a Chinese AI company specialising in facial recognition software was **identified** as part of the CMIC and thereafter, in the same month, another eight Chinese technology companies were so **identified**.

Audit-related security trading prohibition

In December 2020, the **Holding Foreign Companies Accountable Act** (HFCAA) was passed, which enables the US Securities and Exchange Commission (SEC) to prohibit the trading of securities of foreign companies listed on US stock exchanges if the company is unable to submit to audit due to legislation in their country of origin. Two Chinese technology companies were **identified** to be delisted if they failed to submit an audit for three years in a row. On 26 August 2022, China and the United States agreed a deal on audit disputes, opening access to the Public Company Accounting Oversight Board of the United States (PCAOB) to inspect China and Hong Kong-based accounting firms. On 15 December 2022, PCAOB announced that it was able to secure complete access to inspect and investigate audit firms in China "for the first time in history", which has been perceived by the market as elimination of delisting risks for Chinese companies under the HFCAA.

The restrictive measures by the United States raise compliance-related questions for non-US companies. Common challenges are determining what level of due diligence is most appropriate to protect against engaging in or facilitating sanctioned or prohibited trade, and simply keeping abreast of the legacy Trump and continually introduced Biden measures with respect to China.

China's reaction

In response to the challenges caused by US sanctions, China announced an Unreliable Entity List (UEL) in May 2019, and introduced a new blocking statute in early January 2021 and a new Anti-Foreign Sanctions Law in June 2021. In addition, it introduced the Data Security Law, which took effect on 1 September 2021 and the Personal Information Protection Law (PIPL), which took effect on 1 November 2021. The Data Security Law governs "important data", which is subject to export restrictions and prior consent is required for provision of the same to foreign judicial or enforcement authorities. The PIPL also imposes restrictions on the export of data in certain circumstances including the requirement for a security assessment / institutional approval, especially with respect to critical information infrastructure operators (CIIOs) and large-scale data operators. For more, see **section 5** and our briefings **PRC Data Security Law – A New Milestone in Data Legislation** and **PRC Passes Milestone Legislation for Personal Information Protection**.

Unreliable Entity List

The UEL was **announced** in May 2019. Implementing regulations and the actual list were not issued at the time. Based on the announcement by the Chinese Ministry of Commerce (MOFCOM) at the time, it appeared that Chinese market access could be limited for companies and individuals on the UEL. The announcement has since been formalised in September 2020 when MOFCOM published **Order No. 4 of 2020**. The order has made clear that foreign persons who endanger the national sovereignty, security or development interests of China, or suspend normal market transactions with or apply discriminatory measures against Chinese persons, may be added to the UEL. It also clarifies that not only may exports from or imports to China be prohibited or restricted, but also investment in China and personnel entering or staying in China. In addition, fines may be imposed. The actual list and detailed implementation rules have yet to be released.

Export Control Law

Concerning export control, not only is the UEL relevant, but also the **Export Control Law (ECL)** which took effect on 1 December 2020. The now consolidated export control regime applies to "controlled items" which are defined to include dual use items that can be used for both civil and military purposes, military items and nuclear items, and other items related to safeguarding national security and interests, and performing non-proliferation and other international obligations, as well as technical data related to such items. Controlled goods, services and technologies may be contained in published catalogues / lists or subject to temporary control for up to two years. Beyond listed and temporarily controlled items, items that can be used to impair national security and interests, or that can be used to develop or produce weapons of mass destruction or their means of delivery, or that may be used for terrorism purposes are also subject to ECL restrictions.

As to the scope of the ECL in terms of the meaning of export, it refers not only to transfer of controlled items from within to outside China, but also provision of controlled items by Chinese persons to foreign persons whether within or outside China. In addition, the ECL covers transit, trans-shipment and re-export.

The export of certain controlled items may be prohibited altogether, but otherwise exporters wishing to export controlled items must obtain the relevant licence, submit an end use certificate by the end user or by the government authority in the country in which the end user is located, and report any change in use.

The ECL is pertinent to the tech industry, as originating from the Foreign Trade Law, relevant dual use technologies such as encryption, unmanned aerial vehicles and digital computer items have been subject to export control. The establishment of export control compliance programmes is encouraged and guidance has been issued by way of the MOFCOM Guiding Opinions on Establishing an Internal Compliance Programme for Export Control by Exporters of Dual-Use Items.

Blocking Statute
With respect to MOFCOM Rules on Counteracting Unjustified Extra-territorial Application of Foreign Legislation and Other Measures, i.e. China's "Blocking Statute", although it does not clearly state so, a reasonable interpretation is that it only binds Chinese parties. Multinational companies' subsidiaries incorporated in China are clearly bound by the blocking statute. Their branches in China might also be captured, but this is less clear.

China's blocking statute itself does not designate any foreign law as "blocked". Instead, it sets up a framework under which MOFCOM would review and issue prohibition orders against particular foreign laws. While secondary sanctions appear to be the primary target of these new rules, the language has been drafted sufficiently broadly to be able to capture other types of restrictive measures.

If MOFCOM issues a prohibition order against any foreign law, Chinese parties would be required not to comply with the foreign law, unless they receive an exemption from MOFCOM. The potential liability from violating a prohibition order may arise through two possible avenues: civil litigation and administrative penalties. For more, see our briefing **China Issues "Blocking Statute"**.

Anti-Foreign Sanctions Law
Regarding the Anti-Foreign Sanctions Law (AFSL), it provides structure to the ad hoc sanctions already imposed by the PRC government on foreign individuals and entities, and sets out an overarching framework for further developing a legal toolkit for China to resist foreign sanctions. Different from the Blocking Statute, the AFSL is expected to primarily focus on countering foreign sanctions imposed on Chinese officials, state organs and organisations for the purpose of "interfering with China's internal affairs".

The AFSL authorises PRC government agencies to designate foreign individuals and organisations and their affiliates to a Counter List, which may result in denial of visa, freezing of assets and prohibition of parties in the PRC from dealing with those on the Counter List. By way of example, in December 2021, the PRC government imposed **reciprocal sanctions on five US individuals** (in response to US sanctions against five Chinese officials based in Hong Kong in July 2021) pursuant to the AFSL. In the same month, it also imposed **reciprocal sanctions on another four US individuals** in response to US sanctions against four Chinese officials over perceived activity in Xinjiang.

The AFSL also imposes a general obligation on any parties not to "implement or assist in the implementation of discriminatory restrictive measures taken by any foreign country against any Chinese citizens or organisations", whilst its exact scope is subject to further clarification from the PRC government. For more, see our briefing **China Introduces Anti-Foreign Sanctions Law**.

China's sanctions against the United States in light of Pelosi's visit to Taiwan
On 2 August 2022, US House of Representatives Speaker Nancy Pelosi visited Taiwan despite China's serious objection. In response, the PRC Ministry of Foreign Affairs announced the following countermeasures on 5 August 2022: (i) sanctions against Nancy Pelosi and her direct lineal family members pursuant to relevant PRC laws; and

(ii) suspension of co-operation with the United States on a range of issues, including military, defence, repatriation of illegal immigrants, judicial assistance, transnational crime, prohibition of drugs and climate change.

Sanctions in response to developments in Ukraine

The sanctions (including by jurisdictions in APAC, Australia, Japan and Singapore) in response to developments in Ukraine are complex, multilateral and continuing to be incrementally changed in real time in response to developments on the ground. They affect various industries and sectors including the technology industry.

For example, Singapore has prohibited exports of specified dual use goods in the categories of computers, telecommunications and electronics to Russia. With respect to financial measures affecting the technology industry, digital payment token service providers are prohibited in Singapore from facilitating transactions that can aid the circumvention of relevant financial measures.

Japan has similarly prohibited exports contributing to Russian military capabilities including of semiconductors, personal computers and communication devices to Russia. As to cryptoassets, Japan has prohibited the receipt of payments (including by way of cryptoassets) relating to the export of goods contributing to the strengthening of Russia's military capabilities. It has also requested registered cryptoasset exchange service operators to cease processing transfers to those who are Japanese Sanctioned Targets (those that are the target of asset freezes), and to file and report identified cryptoasset trades to Japanese Sanctioned Targets.

Further, recent developments in Australia have prohibited the supply, sale or transfer of 'personal consumer electronics' which exceed AU$500 per unit to Russia, for use in Russia or for the benefit of Russia. Services relating to such a supply, sale or transfer, including technical advice, assistance or training, financial assistance or a financial service are also likely to be prohibited without a valid permit. In addition, it may constitute a contravention of Australian sanctions laws to make a cryptocurrency or other digital asset available to individuals or entities which have been subjected to targeted financial sanctions in response to the Russia-Ukraine conflict. While currently untested, the trading of digital assets issued by certain Russian financial institutions in particular circumstances may constitute a contravention of Australian sanctions laws.

Our team of experts is monitoring the situation closely. For more, see our **Sanctions Topic Guide**.

TECHNOLOGY AND ANTITRUST

9. TECHNOLOGY AND ANTITRUST

9.1 New legislation targeting Big Tech

The debate about how to regulate and ensure "digital" competition and guarantee a fair market is a global one. Jurisdictions around the world have been grappling with how to handle the new tech environment. There is a particular focus upon whether large corporations are engaging in exclusionary or other anti-competitive behaviour which is creating barriers to entry or expansion by new entrants.

The regulators have concerns that existing antitrust laws are not well-suited to deal with the issues arising from the digital economy. Accordingly, new tools have been introduced. Together with other jurisdictions in the world, APAC legislatures are increasingly looking to introduce specific legislation and guidance targeting the digital market and tech giants. Examples are set out below:

- **Korea** amended its Telecommunications Business Act in 2021 to impose restrictions on how app market operators may deal with app developers, other content providers and users. In addition, the amended Monopoly Regulation and Fair Trade Act and the amended Guidelines on Merger Filing took effect on 30 December 2021, such that companies operating social media or digital content with at least 1 million monthly users or significant research and development activities in South Korea must notify all transactions with a value greater than 600 billion won.

- **Japan** introduced the Headquarters for Digital Market Competition in 2019 and introduced the Act on Improving Transparency and Fairness of Digital Platforms in 2021, regulating the behaviour of large online mall operators and app store operators. On 25 April 2022, the Japan Government's Headquarters for Digital Market Competition published an interim report on the competition assessment of the mobile ecosystem, raising issues in relation to 27 types of conduct that may require further consideration and regulation. On 28 June 2022, the Japan Fair Trade Commission published a report on its cloud services survey.

- **China** published in 2021 the Anti-Monopoly Guidelines for the Platform Economy, providing specific guidance on antitrust matters relating to internet platforms, including introducing unique features for analysing and defining the market, capturing the use of algorithms to achieve collusion, and detailing the types of agreements that constitute a violation in the platform economy. In addition, the PRC Anti-monopoly Law was amended in 2022. The newly added Article 9 explicitly prohibits undertakings from using data, algorithms, technologies, capital advantages or platform rules to carry out anti-competitive conduct. For more information, see our briefing **China Passed Amendments to its Anti-Monopoly Law**.

- **Singapore** completed its market study on e-commerce platforms in 2020. Taking into account the findings and recommendations of such market study, the Competition and Consumer Commission of Singapore has proposed to make changes to its various guidelines.

"We predict the trend of conflation of antitrust, privacy and data to continue. Governments around the globe are concerned about the power that accumulated data represents and enacting legislative initiatives around data accordingly."

Sharis A Pozen, Partner, Co-chair, Global Anti-trust Group

- **Australia** launched its five-year inquiry into markets for the supply of digital platform services in 2020. The Australian Competition and Consumer Commission provided its first report in October 2020 and has since provided further reports about every six months with each report focusing on different digital platform services. A series of recommendations have been provided in each report – introducing sector-specific rules is a recurring theme. The final report is due in March 2025.

These initiatives confirm the determination of APAC jurisdictions to address potential antitrust law concerns in a rapidly changing digital economy.

9.2 Increasing investigation and litigation

Antitrust agencies have been hitting hard on Big Tech firms, which have continued to find themselves under increasing scrutiny in relation to their alleged anti-competition behaviour.

In China, within a short period of the guidelines for the platform economy coming into force in early 2021, several prominent platforms were fined for entering into monopolistic agreements or abusing their market position. The review of the concentration of undertakings involving platforms has also been strengthened.

Case Study: Alibaba

Alibaba was engaged in the practice of "picking one from two" whereby online merchants were compelled to choose only one online platform as their exclusive distribution channel.

The State Administration for Market Regulation (SAMR) considered the relevant product market to be that for online retail platforms and found that Alibaba is a dominant online retail platform in China.

SAMR concluded that Alibaba had abused its dominant position by (i) prohibiting some of its platform merchants from opening stores and participating in promotional activities on competing platforms, both explicitly in agreements and verbally; and (ii) putting in place incentive and penalty measures in case of compliance and non-compliance with the exclusivity requirements.

SAMR highlighted the technical aspects of Alibaba's incentive/penalty measures, which were implemented through online traffic volume control, manipulation of search ranking, and supply/refusal to supply promotion resources, mixing the use of platform rules, data and algorithms.

On 10 April 2021, SAMR imposed a record fine of RMB 18.228 billion (approximately US$2.8 billion) on Alibaba for abuse of market dominance.

Antitrust issues, however, do not only concern the Big Tech firms. Changes in technology are occurring so rapidly that even recent "disruptors" are having their business models disrupted. Where future disruption of existing business models is foreseeable, incumbents are increasingly collaborating to create or exploit the new

technology, rather than cede ground to a third party. These types of competitive responses can also raise complex antitrust issues:

- Many online platforms are being investigated by competition agencies for price parity (or "*most favoured nation*") clauses in their contracts with business users of their platforms where the clauses may prevent the businesses from offering better prices to consumers whether on competing platforms or offline.
- Antitrust laws may also inhibit the ability of businesses to profit from proprietary data about their users. Where such data cannot be easily replicated, third parties may seek access to develop their own products or services.
- Self-learning pricing algorithms, and their potential to collude or facilitate collusion, are of continued interest to regulators.

Going forward, we predict the following trends:

1. continuing specific and targeted legislative action to tackle challenges, and the application of antitrust rules in a digitalised world;
2. even more antitrust enforcement against Big Tech firms building on the numerous lawsuits and private actions filed around the globe;
3. growth in antitrust litigation in the tech space;
4. continued scrutiny of Tech M&A and further merger litigation by enforcement agencies;
5. greater focus by antitrust authorities on the use of technologies such as algorithms, machine learning and blockchain, and reviews of potential anti-competitive conduct in industries that use these technologies; and
6. the conflation of antitrust, privacy and data. Governments around the globe are enacting legislative initiatives around data and are concerned about the power that accumulated data represents.

RESPONSIBLE TECH

10. RESPONSIBLE TECH

Political, regulatory and consumer demand for ethical business practices and responsible innovation is greater than ever. We have seen rapid development in ESG reporting and disclosures, and significant ESG investment. Into the future, we will see companies and governments using data and technology to advance their ESG objectives and digital ethics becoming ever more central to product and process design.

10.1 Trends in Responsible Tech

Digital ethics: In an increasingly digital world, businesses are navigating how best to embed ethical principles into their processes, products and services. Principles such as fairness, transparency, accountability, access and explainability will remain a focus in data protection and cybersecurity – as will priority areas for targeted laws and guidance (such as codes for processing children's data or laws on the use of facial recognition technology). These principles will also be the focus in regulatory enforcement and civil litigation. They will be expanded upon in emerging regulation in areas such as online harms, AI and responsible supply chains. Technology developers and providers should increasingly be mindful of, and reactive to, end user interactions, misuse and societal impact – particularly addressing circumstances that can undermine human rights, promote disinformation or facilitate or incite illegal or harmful behaviour. The increasing number and tightening of rules on ethical sourcing will see companies examining supply chain visibility and management in relation to a broad range of matters – from raw materials purchasing, to carbon footprint, to responsible labour practices – both as purchasers and, often, as suppliers themselves. The combination of regulatory pressure, litigation risk and public awareness will make ethical considerations key in tech design, due diligence, governance processes and data use.

Climate tech: COP26 commitments, public funding and heightened investor attention to ESG initiatives will drive innovation in climate tech. We will see the rise of "electrification bundles", which will facilitate the adoption of more sustainability-focused technology for the home, such as rooftop solar, heat pumps and smart power devices. In the automotive industry, more battery electric vehicles (BEVs) and other vehicles seeking to be green will enter the market, with importance placed on new technologies increasing the range and efficiency of batteries and shortening charging times, and tech providing solutions for after-life uses and the recycling of batteries. Carbon capture technology, long-duration storage, agri-tech in farming, circular economy tech and green proptech are all areas to watch. Climate tech companies in these fields and beyond, with their increasing moats in talent pools and intellectual property, strong market currency and growing financing options, will be a focus for M&A activity in the year, and the decade, ahead – with potentially world-changing results.

Infratech: We will see a game-changing reimagining of how energy transition can be achieved through the integration of technology with infrastructure. The resilience of critical infrastructure is a priority for governments across the world as they look to "build back better" from the global pandemic and prepare strategies to achieve their climate targets. The integration of technologies such as smart wires, long duration storage, and even blockchain and other DLTs, with infrastructure will be key to the delivery of sustainable infrastructure for a low-carbon future. Across the energy sector, developers will seek to leverage technology to help decentralise energy distribution, create more

efficient energy networks and provide demand response services linked to electricity usage and supply forecasting. To facilitate the integration of technology with infrastructure, we will see continued investment in autonomous vehicles, data centres, technologies such as 6G (currently being planned), satellite communications and the Cloud, which has become an integral part of IT systems worldwide.

Sustainable finance: Sustainable finance will continue to surge, and technology companies will step in to help with the harnessing of ESG data and to unlock potential sources of liquidity. Reporting and disclosure requirements are driving increasing volumes of ESG data publishing and measurement. With "greenwashing" remaining high on regulators' agendas, accurate, digestible ESG data will be crucial to both bond issuers and investors alike. Platforms using technology such as scraping and machine learning to assist with the extraction, collation and analysis of ESG data will be in high demand. We may also see an increased use of asset tokenisation (the conversion of hard infrastructure assets such as buildings or power stations into digital assets through the use of DLT-based tokens), which has the potential to unlock new sources of finance, particularly for projects in the developing world.

10.2 Increasing reporting, investigations and litigation

All businesses and, in particular, listed entities will face increasing reporting and auditing requirements as global ESG regulations evolve. The Taskforce for Climate-Related Disclosures along with the International Sustainability Standards Board will soon implement a baseline of sustainability standards, that will then be adopted by local standards boards in countries in APAC.

Disclosures in annual reports, announcements and other media will be measured against an increasing set of data points, based on both a company's own performance and those of its competitors. Companies that publish their KPIs on ESG-related issues will be held to those measures. With litigation being used as an enforcement tool by both regulators and private litigants, the stakes will be high.

With COP26 having taken place in November 2021, there will continue to be an increasing focus on ESG considerations across the financial sector. From the environmental concerns of DLT, such as excessive energy consumption and hazardous electronic waste, to social and governance concerns of DLT including facilitating crime such as ransomware attacks and the laundering of illicit funds, as well as ethical issues raised by utilisation of personal data and/or AI, ESG issues surrounding fintech abound. Diversity and inclusion will be key. With an increasing focus on governance, financial firms will need to put in place documented procedures in the development, implementation and use of tech. Whilst firms will increasingly be held to account on ESG issues, on the flip side, this means better opportunities for green or socially aware fintechs. Technologies such as DLT also have the potential to be ESG enablers, accelerating access to the financial system for those who cannot access the same due to social or economic reasons, for example, through government-issued virtual currencies and stablecoins. For more, see our **Talking Tech article on the impact of ESG on DLT**.

10.3 Recent publications

For more, see our publications Ready, Steady, Grow – Building a Sustainable Tech Strategy for the Next Decade; Data Poses the Biggest Ethical Challenge for Organisations, Clifford Chance and Forbes Insights Report Reveals; Big Data Ethics – Charting a Course Through your Data Lake; Safeguarding the Use of AI in the Insurance Sector; The Impact of ESG on Emerging DLT Technologies; Sustainable Digital Finance: How Technology Can Accelerate the Transition to a Sustainable Economy; How Data and DLT Can Accelerate Sustainable Finance; Ethereum Merge – What is at Stake?; The Role of Tech in Trade Policy and Climate Change; Energy Transition Trends 2022; and ESG: Trends to Watch in 2022.

FINTECH

11. FINTECH

What is Fintech?

Fintech encompasses a range of financial services and products that intersect with technology and has rapidly gained momentum in recent years. These include peer-to-peer (P2P) lending, online payments and foreign exchange services, digital wallets and e-money, automated or robo investment advice, cryptocurrencies, non-fungible tokens (known as NFTs) and many more.

Fintech products and services are attractive for their potential to:

- increase efficiency and reduce costs;
- improve access to, and delivery of, financial services;
- enhance the customer experience; and
- create markets in new and innovative financial services products.

Fintech also generates risks, including the potential for money laundering, as well as cybersecurity, consumer protection and data privacy risks.

As financial institutions, regulators and challenger companies embrace the opportunities offered by fintech, it is important to be responsive to the evolving and dynamic nature of these developments.

Regulation of Fintechs

The fintech markets in countries across Asia Pacific are diverse, and regulatory approaches and appetites vary across the region. Generally, regulation is aimed at promoting financial consumer and investor trust and confidence, ensuring markets operate in a fair, efficient and transparent way, and mitigating systemic risks.

The dynamic nature of fintech necessitates that regulatory developments be flexible and adaptable to the speed and content of change. Common regulatory programmes include:

- **regulatory sandboxes**, where eligible start-ups are able to test the viability of their products and services with relaxation of usual regulatory requirements;
- **innovation hubs**, being points of engagement with fintech entrepreneurs that encourage monitoring and understanding of new technologies by regulators;
- **developing guidance principles**, that establish the regulatory approach to developments; and
- **new systems and processes**, used to assess and monitor new developments.

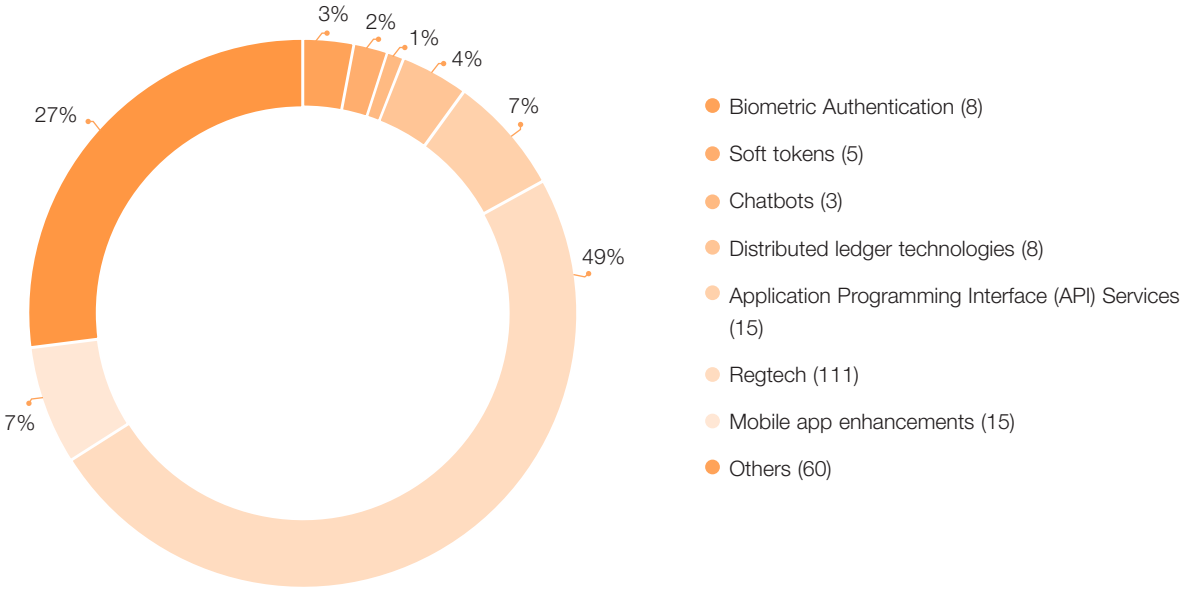
Case Study: Sandboxes

Hong Kong

The HKMA's sandbox allows banks to conduct pilot trials of their fintech initiatives with involvement of a limited number of customers and without the need to fully comply with supervisory requirements.

As of September 2021, the HKMA's sandbox had tested 225 fintech initiatives in the following areas[13]:

Distribution of technologies involved in pilot trials
(as of end-September 2021)



Total: 225 cases

Similarly, the IA has established a sandbox for authorised insurers to facilitate a pilot run of fintech and an Insurtech Facilitation team to enhance communication with businesses involved in the development and application of fintech.

In terms of cross-boundary fintech initiatives, the HKMA and the People's Bank of China signed a MOU in October 2021 to provide for a one-stop supervisory sandbox platform to allow financial institutions to conduct pilot trials concurrently in Hong Kong and Greater Bay Area cities. The HKMA (as well as the SFC and IA) are also members of the Global Financial Innovation Network, which was formed to provide a more efficient way to interact with financial services regulators worldwide and to which firms can apply to conduct cross-border tests of innovative financial products or services.

Singapore

In Singapore, the MAS FinTech Regulatory Sandbox provides FIs and FinTech players a live environment to experiment with innovative financial products or services. MAS provides regulatory support by relaxing legal and regulatory requirements prescribed by

13 HKMA Fintech Supervisory Sandbox webpage, https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/

MAS. The sandbox includes appropriate safeguards to contain the consequences of failure to maintain the stability of the financial system.

Regulation of Cryptocurrency and NFTs

Regulatory approaches are also dependent on the fintech in question. Two types of fintech which demonstrate the uneven landscape of fintech are cryptocurrency and NFTs.

Cryptocurrencies and virtual assets under the regulatory microscope

The substantial growth of trading in Bitcoin and other cryptocurrencies has intensified regulators' attention on what many trading commodities consider to be a new asset class. Initial coin offerings (known as ICOs) – the selling of digital tokens in exchange for capital including virtual currency such as Bitcoin – pose a particular risk for unwary investors. Uncertainty about how they should be regulated means inconsistent protection under securities laws. Online fundraisings are subject to the potential of internet fraud, including phishing scams, the publication of fake news items that may drive up the price, and the possibility of the hacking of the underlying software.

Regulators throughout APAC have acted. On 4 September 2017, China declared that ICOs were illegal and called a halt to fundraising involving virtual coins. Since 2017, supervisory enforcement action by PRC regulators against cryptocurrency-related business activities within the PRC has been enhanced. The latest regulations reaffirm that the following activities are contrary to law: (i) undertaking business for conversion between cryptocurrency and fiat money, or conversion between various cryptocurrencies; (ii) buying and selling cryptocurrencies as a central counterparty; (iii) providing information intermediary and pricing services for cryptocurrency transactions; and (iv) engaging in ICO and cryptocurrency derivatives transactions.

The SFC in Hong Kong issued a statement on 5 September 2017 noting that digital tokens offered in ICOs may be securities and subject to securities laws in Hong Kong; this was followed by a number of statements (in February and March 2018, and March 2019) in which the SFC reported its action in warning and halting certain ICOs, and reminded the public of the risks in ICOs or security token offerings (STOs).

More recently, in July 2021, the SFC published a warning statement to both investors trading virtual assets on unregulated platforms and intermediaries intending to provide financial services in virtual assets, noting specifically that Binance, one of the most popular cryptocurrency exchanges globally, has offered trading services in Stock Tokens in a number of jurisdictions. Stock tokens are virtual assets that are represented to be backed by depository portfolios of underlying, overseas-listed stocks; they are promoted as a means for investors to purchase fractional shares and are likely to be securities as defined in the SFO. The SFC expressed concerns that these services may be offered to Hong Kong investors without the platform being licensed or registered to conduct regulated activity in Hong Kong. The SFC reiterated that it would not hesitate to take enforcement action against unlicensed platform operators where appropriate. Similarly, in August 2021, the SFC warned against unauthorised collective investment schemes and investment arrangements involving digital tokens and ICOs, which should be taken up with extreme caution due to the associated risks.

Hong Kong is further in the process of introducing robust licensing requirements for virtual asset trading platforms (also referred to as cryptocurrency exchanges), which puts Hong Kong (together with Singapore) at the forefront of this area.

Despite the risks, Hong Kong was ranked as the leading jurisdiction for token offerings globally in 2019 (as at 31 October 2019) by total funds raised and this included the third biggest token offering globally since 2016 (by Bitfinex, raising US$1 billion) according to a joint report by PricewaterhouseCoopers and Crypto Valley[14].

ICOs have also come under regulatory scrutiny in Singapore. In May 2018, the MAS warned eight digital exchanges in Singapore not to facilitate trading in digital tokens that are securities or futures contracts without MAS authorisation. It also warned an ICO issuer to stop the offering of its digital tokens in Singapore as its tokens represented equity ownership in a company, and were, therefore, considered as securities under the Securities and Futures Act 2001 (SFA). The issuer ceased the offer, returned all funds received from Singapore-based investors and took remedial actions to comply with MAS regulations. As for cryptocurrencies, there have been multiple consumer advisories to warn the public of the risks of trading such products. From the regulation standpoint, the Minister-in-charge of the MAS clarified on 5 April 2021 that exchanges offering the trading of cryptocurrencies are regulated as digital payment token service providers under Singapore's Payment Services Act. For securities tokens, they are subject to the same securities legislation as traditional securities – i.e., the SFA.

In Australia, the Australian Securities and Investments Commission has issued regulatory guidance (Information Sheet 225) to assist businesses with understanding their obligations under the Corporations Act 2001 (Cth), the Australian Securities and Investment Commission Act 2001 (Cth), and other Australian laws in connection with cryptoassets and ICOs.

On 27 October 2017, the Financial Services Agency of Japan (FSA) released a statement to remind the public of the risks involved in ICOs, as well as noting that ICOs may be subject to Japanese regulations, including the Payment Services Act (Act No. 59 of 2009, as amended) (PSA) and the Financial Instruments and Exchange Act (Act No. 25 of 1948, as amended) (FIEA). Certain digital tokens fall within the definition of cryptoassets, and acts including the exchange of such cryptoassets, are regulated under the PSA. Also, on 1 May 2020, amendments to the PSA and the FIEA came into effect, clarifying that cryptoassets and tokens offered in exchange for cryptoassets are regulated under the FIEA. In order to avoid an overlap of regulations, the amendments also specify which types of tokens offered in ICOs are regulated under the FIEA and which types of tokens may otherwise be regulated under the PSA.

For more, see our briefing **Security Token Offerings – The Shape of Regulation Across Asia-Pacific**. For the EU position, see **MiCA – EU Reaches Agreement on the Crypto-assets Regulation**. For the global position on the Ethereum Merge, see **Ethereum Merge – What is at Stake**?

14 PricewaterhouseCoopers & Crypto Valley, 6th ICO / STO Report – A Strategic Perspective, Spring 2020, https://www.pwc.ch/en/publications/2020/Strategy&_ICO_STO_Study_Version_Spring_2020.pdf

Case Study: Hong Kong Virtual Asset Regulation

The SFC in Hong Kong has adopted a technology neutral regulatory approach and seeks to regulate virtual assets and related activities based on the existing legislative framework, and the intrinsic characteristics of the relevant activities and risks arising from them.

Where virtual assets fall under the definition of "securities" or "futures contracts" under the Securities and Futures Ordinance (SFO), such assets and related activities will fall within the SFC's ambit (albeit the latest January 2022 circular also gives guidance on virtual asset dealing services irrespective of whether the virtual assets involved are securities). STOs are typically structured to have the features of traditional securities offerings but involve digital representations of the ownership of assets or economic rights utilising distributed ledger technology (DLT) or other digital infrastructure.

Firms offering security tokens should consider the nature and features of the tokens being offered to determine whether the tokens are securities or another type of regulated instrument, and ensure they comply with applicable product authorisation and licensing requirements under the SFO, as they do when offering other types of securities.

Distribution of Virtual Asset Products and Dealing and Advisory Services

In November 2018, the SFC specifically brought some virtual asset activities in which the investing public are involved within its regulatory net under existing powers. SFC-licensed portfolio managers which intend to invest 10% or more of the gross asset value of the portfolio in virtual assets need to observe additional requirements as part of their licensing conditions. In October 2019, the SFC developed a set of standard terms and conditions for virtual asset portfolio managers, which may be adapted depending on their business model and are generally appropriate to be imposed as licensing conditions (for example, allowing only professional investors to invest, assessment of investor knowledge of virtual assets, ensuring that the amount invested is reasonable in light of the client's net worth, providing specified information to clients, and risk management of the virtual asset fund).

In November 2018, the SFC also set out the expected standards for licensed corporations which distribute virtual asset funds. In the SFC's March 2019 statement on STOs, it stated that it considered security tokens as complex products with complex products being subject to additional investor protection measures, including those specified in the Guidelines on Online Distribution and Advisory Platforms effective July 2019 and paragraph 5.5 of the Code of Conduct for Persons Licensed or Registered with the SFC.

The November 2018 circular has now been superseded by the comprehensive January 2022 circular jointly issued by the SFC and the HKMA. The January 2022 circular covers the distribution of virtual asset-related products and provision of virtual asset dealing and advisory services. Virtual asset-related products are defined as those having a principal investment objective or strategy to invest in virtual assets; deriving their value principally from the value and characteristics of virtual assets; or tracking or replicating investment results or returns which closely match or correspond to virtual assets.

The January 2022 circular clarifies and extends earlier requirements. For the distribution of virtual asset-related products, they are likely to be considered complex products and if so, requirements such as suitability (irrespective of whether there has been a solicitation or recommendation), and the provision of minimum information and warning statements (examples are contained in appendix 5 to the circular) apply. Further, if considered complex products, they should only be offered to professional investors; excepted products include virtual asset derivative products traded on specified regulated exchanges, or authorised or approved exchange-traded virtual asset derivative funds. Even professional investors which are not institutional or qualified corporates should have assessed their knowledge of investing in virtual assets and the sufficiency of their net worth to assume relevant risks.

For the provision of virtual asset dealing services, regardless of whether the virtual assets involved are securities, regulatory requirements must be complied with. Intermediaries must partner with SFC-licensed trading platforms (see below on virtual asset exchanges) and may introduce clients to the platform for direct trading or establish an omnibus account with the platform and act as agent to execute instructions. Virtual asset dealing services should only be provided to professional investors. Intermediaries licensed for type 1 securities dealing regulated activities may provide virtual asset dealing services only to existing clients. Where an omnibus account arrangement is used, it will be subject to the licensing conditions in appendix 6 to the circular including clients only being permitted to deposit or withdraw fiat currencies (and not virtual assets) from their accounts. Where discretionary account management services are being provided (by type 9 asset management intermediaries) and there is an intention to invest 10% or more of the gross asset value of the portfolio in virtual assets, they continue to be subject to additional requirements as part of licensing conditions as set out in the October 2019 pro forma terms and conditions discussed above. Type 1 intermediaries providing such services on an ancillary basis should only invest less than 10% of the gross asset value of the portfolio.

Requirements for the provision of virtual asset advisory services are a mix of those for distribution of virtual asset-related products and provision of virtual asset dealing services.

At the same time, the HKMA issued a circular providing guidance to authorised institutions with customers engaging in virtual asset-related activities through their bank accounts, business relationships with virtual asset service providers, and investment in virtual assets. The guidance is for a risk-based approach to be adopted including undertaking risk assessments and appropriate mitigation measures based on legal and regulatory requirements, and for sufficient senior management oversight. Risk areas highlighted are from a prudential perspective, as well as anti-money laundering (AML), counter-terrorist financing (CTF) and financial crime risks.

Similarly, the IA issued a circular guiding the insurance industry in dealing with virtual assets and related service providers, including to review the Guideline on Enterprise Risk Management (GL 21), Guideline on Cybersecurity (GL 20) and Guideline on AML/CTF (GL 3) in evaluating and addressing risks, and the Guideline on Corporate

Governance of Authorised Insurers (GL 10) in product design and customer treatment involving acceptance of virtual assets as premiums or providing coverage or benefits linked to virtual assets.

The HKMA and IA circulars have the potential to restrict the ability of the banking and insurance industry and their customers to deal with unregulated virtual asset service providers. In view of these circulars and the requirements of the SFC and HKMA joint circular, the role of unregulated (unlicensed or overseas) players is likely to be reduced or they will need to obtain licensing in Hong Kong to serve Hong Kong customers.

Virtual Asset Exchanges
The SFC also set a conceptual framework for virtual asset trading platform operations (or cryptocurrency exchanges) in November 2018. In November 2019, the SFC then issued a position paper providing further clarity on the regulatory framework, which targeted centralised virtual asset trading platforms operating in Hong Kong which traded at least one security token and provided for an opt-in regime. An interested trading platform operator would be placed in the SFC Regulatory Sandbox. As with virtual asset portfolio managers, prescribed terms and conditions / licensing conditions were contained in appendix 1 to the position paper.

2020 saw the first SFC licensing and approval of a virtual asset portfolio manager (Venture Smart Asia Limited), which was also the adviser and distributor to a Hong Kong cryptocurrency fund, and the first SFC licence to a virtual asset trading platform operator (OSL Digital Securities Limited).

Since then, the Financial Services and the Treasury Bureau (FSTB) has carried out a consultation on legislative proposals to enhance the AML/CTF regime and introduce a licensing regime for persons operating a virtual asset exchange in Hong Kong as licensed virtual asset service providers (VASPs) under the AML and CTF Ordinance (Cap 615) (AMLO). Consultation conclusions were published in May 2021. The relevant amendment bill was introduced in the Legislative Council for its first reading in July 2022 and is expected to be passed before the end of 2022. The new regime is proposed to take effect on 1 March 2023. The definition of virtual assets will not include digital representations of fiat currencies, financial assets already regulated under the SFO, or closed-loop limited purpose items that are non-transferable or non-fungible (such as air miles and credit card rewards). Only companies registered in Hong Kong under the Companies Ordinance (Cap 622) (including non-Hong Kong companies incorporated elsewhere) may apply for a VASP licence. Licensed VASPs will be subject to requirements in Schedule 2 to the AMLO including those relating to customer due diligence and record-keeping. The applicant (and at least two of its responsible officers, all of its directors, and its ultimate beneficial owner) will be required to pass a fit and proper test and the SFC will be empowered to impose licensing conditions, as well as regulatory requirements, including those relating to financial resources, segregation and management of client assets, and financial reporting and disclosure. The services of a virtual asset exchange will be confined to professional investors only and such requirement may be imposed as a licence condition (at least in the initial stage of the regime). Persons in Hong Kong or elsewhere will be prohibited from (and it will be an offence to) actively market to the Hong Kong public a regulated virtual asset activity unless the person is a licensed VASP.

Cryptocurrency and virtual asset disputes

Apart from considering how regulators in APAC have dealt with virtual assets, other legal issues to have regard to include whether tokens and virtual assets can be legally transferred effectively, whether security can be granted over them, whether they can be the subject of a trust and, in the event of a breach of trust or fraud, traced. This will depend on whether they legally constitute property.

A New Zealand case has held that cryptocurrencies constitute property. The Singapore Court of Appeal declined to come to a final position on the question in February 2020; however, in an interlocutory decision in March 2022, the High Court held that cryptocurrency can be regarded as property and be the subject of a proprietary injunction, albeit the Court caveated its holding by stating that it did not engage in complex questions of law at the interlocutory stage. For more, see our Talking Tech publications **Using Court Orders to Help Recover Stolen Cryptocurrencies and The Solana Cyber-attack: What Now?** Australian, English and Hong Kong courts have granted proprietary injunctions over cryptocurrency with the English courts doing so expressly on the basis that cryptocurrency is property and an Australian court has allowed cryptocurrency to stand as security for costs. There is also a November 2019 UK Jurisdiction Taskforce Legal Statement on Cryptoassets and Smart Contracts[15] that states cryptoassets are to be treated in principle as property and such statement has been cited in New Zealand and Singapore case law. We would comment, however, that the case law relates to more commonly traded coins such as Bitcoin and Ethereum; it remains to be seen whether novel issues might arise from other coins with novel characteristics.

Another issue is whether an exchange or trading platform is considered to hold virtual assets on trust for their clients.

Such an issue might come into play, for example, if an exchange or trading platform becomes insolvent and the liquidators need to determine whether the virtual assets are part of the insolvent estate available for distribution. See our client briefing **Decoding Distress: Cryptoassets, Restructuring, and Insolvency under English Law**. They might also come into play when there are technical abnormalities, and a dispute arises as to whether disputed trades may be cancelled and, if not, who is entitled to the proceeds.

There has been Singapore and New Zealand case law on this trust relationship issue, and the answer very much depends on the parties' intention as evidenced by the terms and conditions between them and other evidence pointing to their conduct, such as whether the operator traded in its own right, and whether the virtual assets were treated as the operator's own, for example, in the operator's accounts, financial statements and tax returns.

In the Singapore case, the fact that the cryptocurrency exchange segregated its virtual assets from those of customers was not in and of itself sufficient to form a trust relationship. For more on the Singapore case, please see our client briefing **here**.

15 UK Jurisdiction Taskforce, The LawTech Delivery Panel, Legal Statement on Cryptoassets and Smart Contracts, November 2019, https://lawtechuk.io/explore/cryptoasset-and-smart-contract-statement

On the other hand, in the New Zealand case, the relevant cryptocurrency exchange was held to hold digital assets on trust because it had no intention to trade in its own right; it did not allocate to account holders public or private keys to digital wallets and the trusts' beneficiaries were clearly recorded in a database.

Central Bank Digital Currency (CBDC)
Based on the HKMA's role as Hong Kong's central bank, the HKMA was involved in Project Inthanon-Lion Rock with the Bank of Thailand to develop a CBDC prototype based on DLT (blockchain is a type of DLT and is the technology that underpins most cryptocurrency including Bitcoin) and smart contract technology allowing participating banks in both jurisdictions to conduct cross border fund transfers and foreign exchange. The cross-border corridor network prototype built in the first phase has since been developed to support more currencies and interface with domestic payment systems. The phase 2 prototype now enables participating central banks the ability to monitor flows and balances and manage liquidity; enhance the level of privacy of transactions; and automate certain compliance functions. Compared with the current correspondent banking model, the prototype has the potential to speed up cross-border transfers and reduce their costs. The findings from phase 2 were delivered in a report in September 2021. The project is due to enter phase 3 (transition to open-source, production-ready system) and will be known as the Multiple Central Bank Digital Currency Bridge (mBridge) project with the joining of the Hong Kong Centre of the Bank for International Settlements Innovation Hub, Digital Currency Institute of the People's Bank of China and the Central Bank of the United Arab Emirates.

At the retail level, the HKMA has conducted technical and policy market consultations on the prospect of issuing retail CBDC in Hong Kong, to be known as e-HKD. To this end, the HKMA released a technical white paper in October 2021 exploring potential design and architecture options that can be applied to the infrastructure for distributing e-HKD. In terms of design, the HKMA proposes a two-tier system, namely, a wholesale interbank system for the HKMA to issue and redeem CBDC and a retail user wallet system for commercial banks to distribute and circulate retail CBDC or CBDC-backed e-money. The HKMA recognises the need to protect privacy and that if it does not record retail balances, which is instead the responsibility of private sector intermediaries; this will comply with the principle that only necessary data is disclosed to relevant parties. To facilitate the two-tier system, the white paper also unveiled technical architecture in the form of a ground-breaking arrangement that allows transaction traceability in a privacy-friendly manner. Whilst the October 2021 white paper was primarily concerned with the technical aspects of introducing e-HKD, in April 2022, a further discussion paper was published considering policy and design perspectives, examining such challenges as interoperability with other payment systems, privacy and data protection, and cybersecurity, as well as use cases. In September 2022, the HKMA released a position paper entitled "e-HKD: Charting the Next Steps" and confirmed that it will start paving the way for the future introduction of e-HKD.

Meanwhile, in terms of other fintech initiatives by the HKMA, to facilitate access to trade financing and execution of open account contracts, and reduce costs and inefficiencies, the HKMA launched a blockchain-based trade finance platform "eTradeConnect". This combines the services of major domestic and international

banks, to be further linked up with other blockchain platforms including the People's Bank of China Trade Finance Platform. Apart from the benefits from the use of blockchain and DLT, the HKMA also highlighted the legal issues and risks in the Whitepaper 2.0 on DLT in October 2017, such as issues of legal validity and enforceability in the use of digital signatures and smart contracts; data protection and privacy; challenges arising from cross-border transactions; governance concerns and participant liability; and competition and anti-trust issues.

In Singapore, the Managing Director of MAS stated on 9 November 2021 that MAS sees much promise in wholesale CBDCs as they have the potential to radically transform cross-border payments. Project Ubin was started five years ago to experiment with blockchain technology and wholesale CBDCs. This inspired Partior, a blockchain-based interbank clearing and settlement network jointly established by DBS Bank, JP Morgan, and Temasek. Project Ubin also serves as a foundation for Project Dunbar – a blueprint for a multi-currency settlement platform that operates across countries. It would allow commercial banks to transact directly with one another using wholesale CBDCs of their respective countries, eliminating the need for intermediaries. As for retail CBDCs, the MAS launched the Global CBDC Challenge on 28 June 2021 to seek innovative retail CBDC solutions. As for the future, MAS has concluded that despite the benefits that it would bring, the case for a retail CBDC in Singapore is not urgent. The MAS is of the opinion that physical cash is likely to still be used for quite some time. Nevertheless, the MAS is embarking on Project Orchid to build the technology infrastructure and technical competencies necessary should Singapore intend to issue a Singapore CBDC in the future.

For more, see our briefing **Central Bank Digital Currencies and Stablecoins – How Might They Work in Practice?**

Case Study: Facebook Libra / Diem and Stablecoins

Libra was first announced in June 2019, but rebranded as Diem in December 2020. Diem is a stablecoin, a class of cryptocurrency that attempts to offer price stability by being backed by a reserve asset such as a fiat currency, commodity or other cryptocurrency, or by the control of supply through an algorithm.

The stated mission of Diem is to create a simple global payment system that complements existing fiat currencies enabling new functionality, reducing costs and fostering financial inclusion in terms of providing services to the unbanked and underbanked.

However, privacy, consumer protection, monetary policy and national security concerns over Diem have been cited, including by the US House Financial Services Committee, exacerbated by Facebook's involvement and poor record of data protection for its users. For more on the issues raised after Libra's launch, see our **briefing on financial crime risks, briefing on tax complications** and **briefing on challenges generally**. As of September 2021, unease on the part of the US Treasury Department remains , a major concern being a new payment system having the potential to create a financial hazard whereby in circumstances of financial panic – similar to that during the last financial crisis or early days of COVID-19 – people might rush to liquidate their stablecoins and the government will have to decide whether to step in and bail out. Controversies involving Facebook also

continue, such as an antitrust case brought by the US Federal Trade Commission in December 2020

The issues originally raised led to an exodus of members from the Diem Association including Visa, Mastercard, PayPal, eBay and Vodafone, albeit it is still backed by major companies such as Spotify and Uber[16].

The Diem Association has since promised that the project will not advance until approvals from the necessary financial watchdogs are obtained.

Diem will use permissioned blockchain technology with distributed governance by Association members. Whilst there was an intention to transition to a permissionless system in the future, this appears to have been abandoned.

The Diem Association is working with regulators, central bankers, ministers and policymakers, and three key changes have been introduced to address regulatory concerns[17].

- **Offering single-currency stablecoins in addition to the multi-currency coin**
  - There was a concern that a multi-currency coin might interfere with monetary sovereignty and monetary policy. To address this, Diem will offer single-currency stablecoins and launch a pilot with the US dollar, and generally start with stable and liquid currencies such as EUR, GBP and SGD. Each single-currency stablecoin will be fully backed by the Diem Reserve, which will consist of cash or cash equivalents and short-term government securities in that currency. The multi-currency coin will not be a separate digital asset, but a digital composite of some of the single-currency stablecoins, which will be implemented by way of smart contracts. The multi-currency coin can be used for cross-border settlements and as a low-volatility option for people and businesses in countries that do not have a single-currency stablecoin on the network. The intention is to also provide for interoperability and upgradability, including seamless integration with CBDCs as they become available, and provide additional functionality and features for CBDCs.
- **Robust compliance framework**
  - The goal to design a system ensuring compliance with applicable laws and regulations whilst maintaining openness and financial inclusion. Feedback from regulators includes the need to develop a framework and standards for compliance and risk management in relation to AML, sanctions compliance, and the prevention of illicit activities, which network participants are to adhere to. Safeguards for the security and integrity of the Libra payment system will also need to be introduced. There will potentially be four categories of network participants: (i) designated dealers; (ii) regulated VASPs including exchanges and custodial wallets that are registered or licensed in a Financial Action Task Force (FATF) member jurisdiction; (iii) certified VASPs that have completed a certification process approved by the Association; and (iv) other individuals and entities seeking

16 Ryan Browne, CNBC, Facebook-backed Diem aims to launch digital currency pilot later this year, 20 April 2021, https://www.cnbc.com/2021/04/20/facebook-backed-diem-aims-to-launch-digital-currency-pilot-in-2021.html

17 Diem, Whitepaper v2.0, April 2020, https://www.diem.com/en-us/white-paper/

to provide services or transact through the Libra network (unhosted or self-hosted wallets). Initially, the network will be made accessible to designated dealers and regulated VASPs, whilst the Diem Association develops its certification process for other VASPs and a compliance framework for unhosted wallets. For example, unhosted wallets will be subject to balance and transaction limits.

- **Strong protection in the design of the Diem Reserve**
  - Each single-currency stablecoin will be backed 1:1. The Reserve will hold assets of very short-term maturity, low credit risk and high liquidity, and will further maintain a capital buffer. There will also be the support of a network of resellers and exchanges for conversion of Libra coins into local currency.

Whilst Libra foundered, another stablecoin seized the limelight. Tether also promised a 1:1 exchange rate with the US dollar and has issued an estimated US$80 billion over worth of tokens[18]. Supporters of Tether and stablecoins generally say they afford cryptocurrency users a safe way of redeeming their earnings into dollars. They can also be more easily included in blockchain-enabled smart contracts and provide an alternative architecture for digital payments that is more efficient and cheaper than the current structure of, for example, Mastercard and Visa. However, Tether (and stablecoins generally) are facing regulatory scrutiny, with the US Commodity Futures Trading Commission issuing a US$41 million fine for Tether's failure to maintain sufficient monetary reserves between 2016 and 2018. More generally, in July 2021, Secretary of the US Treasury Janet L Yellen convened the President's Working Group on Financial Markets to discuss stablecoins and a report with recommendations for addressing regulatory gaps was issued in November 2021.

Turning to Asia, in a speech by Julia Leung, Deputy Chief Executive Officer of the SFC, during FinTech Week in November 2021, she highlighted in relation to virtual assets that one of the three areas of regulatory attention is stablecoins in light of the explosion of interest in Diem. She referred to the relative stability of stablecoins and the potential to make cross-border payments far less expensive. Subsequently, the HKMA issued a discussion paper regarding stablecoins seeking industry feedback with the aim of introducing a new regime no later than 2024. The HKMA expressed its views recommending a risk-based approach and emphasised that its focus will be on asset-linked stablecoins rather than those that are algorithm-based. It will either expand the scope of the existing Payment Systems and Stored Value Facilities Ordinance or introduce new legislation. Authorisation is proposed to be required: some of the proposed regulatory requirements include adequate capital and liquidity; redemption requirements; fit and proper controllers and management; sound management of AML, cybersecurity and other risks; and financial reporting and disclosure.

Whilst stablecoins have a role to play in making cross-border payments more cost-effective, their future including that of Diem remains to be seen including how regulatory issues will be resolved.

As discussed, blockchain and DLT have the potential to transform how securities are issued, traded and settled. However, the adoption of technology in the capital

18 Alex Hern, The Guardian, Tether to launch stablecoin tied to pounds as UK aims to become crypto hub, 22 June 2022, https://www.theguardian.com/technology/2022/jun/22/tether-stablecoin-tied-to-pound-uk-crypto-currency

markets has not matched take-up in other areas of finance and trade and, so far, has been used only for enhancing existing elements of the process rather than replacing it with something new. We explore the reasons for this and share our experience of some of the developments in this area and other uses of technology in the capital markets in the Talking Tech publication **Are We Set for a Capital Markets Fintech Reinvention**?

The rise of NFTs

Non-fungible tokens (NFTs) – unique cryptoasset "originals" of items such as digital artworks, source code and tweets stored on a blockchain – have skyrocketed in popularity, with regulatory oversight yet to meaningfully catch up anywhere in the Asia Pacific region. The comparatively recent emergence of NFTs when compared with fintech such as cryptocurrency means that there is still debate as to how NFTs can meet existing regulatory expectations, particularly as NFT trading often necessitates the use of cryptocurrency and crypto wallets, which countries such as China have banned. NFTs are also vulnerable to fraud and copyright infringement risks. It is noted that case law (at least in England) is beginning to emerge to address some of these risks, such as a recent March 2022 judgment recognising an arguable case for NFTs to be property at least capable of being the subject of an interim freezing injunction (to freeze misappropriated NFTs).

While Asia Pacific nations continue to explore the impact and implications of the introduction of NFTs to the fintech space, the eventual regulation of NFTs will be influenced by considerations such as:

- whether the NFT itself is a "security" or another regulated product;
- whether NFTs are captured by regulations of virtual asset platforms; and
- whether there are other general regulations and legislative requirements that apply to the NFT as a good or service, such as anti-money laundering and 'know your client' obligations, and misleading and deceptive conduct standards.

In Singapore, the Minister for Communications and Information provided its view on NFTs on 11 January 2022. It stated that new technologies like the Metaverse and NFTs are at a nascent stage of development, and thus it remains to be seen how they will be structured and organised. It clarifies that the Singapore Government is closely studying their characteristics and attendant implications and risk. Despite this, industry players and individual users were encouraged to exercise caution in dealing with NFTs.

Similarly, in June 2022, the SFC in Hong Kong reminded investors of the risks associated with investing in NFTs. Risks cited include illiquid secondary markets, volatility, opaque pricing, hacking and fraud. The SFC acknowledged that activities relating to genuine digital representations of collectibles do not fall within its regulatory ambit. However, what may fall within its regulatory ambit are fractionalised NFTs structured in a form similar to securities or as interests in collective investment schemes. Marketing or distributing or offering to the Hong Kong public participation in a CIS may require a licence or authorisation from the SFC.

For further discussion, see our briefing **Non-Fungible Tokens: The Global Legal Impact**.

Digital trade finance

COVID-19 and consequent disruption to supply chains has accelerated the use of electronic transferable records in international trade finance as an alternative to paper-based transactions. However, the international trade finance community continues to grapple with the gulf that now exists between the opportunities offered by technological developments and what is legally permitted or recognised in respect of that transferable record. Efforts to address that legal reform are outlined in our briefing **Paperless International Trade: Achieving harmony between the law and technological potential**.

What's next?

- An increased use of electronic transferable records as a result of the removal of legal impediments. Countries such as Singapore have now adopted the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Transferable Records (2017) (MLETR). Other countries, such as the UK, are looking at alternative approaches to reform their legal frameworks so as to facilitate recognition of electronic transferable documents. In parallel, efforts are being made to promote and reform the Uniform Rules for Digital Trade Transactions, as well as other eRules. Successful removal of legislative hurdles will need continued co-operation across the international community to ensure that their efforts dovetail to ensure consistency in approach.
- Continued focus on the use of platforms to facilitate trade finance with various international online forums being created, for example, to facilitate the connection of financiers with traders. For the most effective results, these will need to develop and offer:
  - more inter-platform API (Application Programming Interface) connectivity and partnerships to counter the emergence of "digital islands" by ensuring cohesion and integration of end-to end paperless trade processes including financing, logistics, customs and insurance;
  - the embedding of regtech Solutions for 'know your customer', anti-money laundering and other compliance and regulatory requirements;
  - counterparty verification (through the adoption of verifiable legal entity identifiers (LEIs) or alternatives) in onboarding for more streamlined risk management in eradicating fraud while accelerating payments and goods flows.
- Greater development of data highways linking transport hubs, customs departments and logistics players with banks and insurers in order to facilitate sustainable supply chains and wider governance. The instantaneous exchange of connected data streams is widely recognised as being important for reducing administration and bureaucracy and enabling large trade flows.

Implications for Financial Institutions

Given the rapid growth of fintech, financial institutions face three options:

- building their own organic fintech capabilities;
- acquire fintech businesses; or
- collaborate with fintech providers through joint ventures, partnerships, outsourcing or white label arrangements.

Often, banks seek collaboration with fintech providers to deepen their product offerings and improve customer satisfaction without the cost and risk associated with developing all solutions in-house or acquiring and integrating a business. Potential risks associated with this approach are the allocation of liabilities between a smaller and a much larger organisation; the allocation of risks and rewards; antitrust concerns; the contribution, sharing, ownership, access and use of IP and data; and cyber, data and infringement risks.

This kind of collaboration leads to legal challenges, such as the use of APIs, which companies like banks are using to allow third parties to access their data or services in a controlled environment. Despite the challenges, APIs bring opportunities particularly given the widespread move to digitalisation as further accelerated by COVID-19.

Case Study: Open Banking and API in Hong Kong and Singapore

Open banking allows third-party service providers to have access to banks' product, service and process information, and customers' account, payment and transaction information held by their banks, which is done through an API.

In Hong Kong, the HKMA introduced an Open API Framework for the banking sector in July 2018. Phases I and II were launched in January and October 2019 with banks offering access to their product and service information and customer acquisition processes, respectively.

To further encourage the adoption of Open API, the Common Baseline, a set of applicable business and risk management considerations to be negotiated between a bank and an onboarding third-party service provider, was also released in November 2019. More than 800 Open APIs have been launched under Phases I and II.

Phases III and IV relating to the retrieval and alteration of customer account information and payment and banking transactions are being implemented progressively from December 2021. This is being accompanied by technical and operational standards in areas such as customer authentication and data security by way of refinement of the Common Baseline.

The first use cases to be implemented under Phases III and IV relate to deposit account information and app payment functions.

Singapore has also been touted as a leader in the Asia Pacific of open banking according to the Open Banking APAC report by the Emerging Payments Association Asia (EPAA) released in February 2020. The MAS has contributed to this by publishing an API playbook which serves as a comprehensive guideline for FIs and FinTech firms to develop and adopt open API-based system architecture within their organisations. In November 2018, MAS introduced API Exchange (APIX), the world's first cross-border, open architecture platform. APIX allows FIs and FinTech firms to connect and collaborate on design experiences via APIs. Additionally, the MAS operates the Financial Industry API register, which tracks open APIs in the Singapore financial industry by functional categories. MAS follows a voluntary adoption approach and banks in Singapore like DBS, Standard Chartered and UOB have leveraged API technology to enhance their services.

Fintech Trends to Watch

- Regulators will continue to work on bringing cryptoassets within the regulatory perimeter including tightening of AML regulatory requirements – for example, Hong Kong's bill to introduce a licensing regime for VASPs as discussed above – as well as requirements around advertising, marketing and promotion to the public including the Monetary Authority of Singapore's January 2022 Guidelines to Discourage Cryptocurrency Trading by General Public. For more on crypto regulation in the US and UK, see our publications **Biden Signs Crypto Executive Order; New York Department of Financial Services (NYDFS) Flexes Enforcement Muscle in Crypto Markets with $30 Million AML and Cybersecurity Fine and Draft Cybersecurity Amendments**; **OFAC Urges the Virtual Currency Industry to Get Real about Sanctions Compliance**; **Cryptoasset Advertising – ASA Publishes New Rulings for Cryptocurrency Marketing**; and **Are We Still Allowed to Talk Crypto? – New Proposals for the Regulation of Cryptoasset Promotions**.
- The rise of decentralised finance (DeFi) which aspires to create a global peer-to-peer alternative to traditional finance using permissionless DLT or blockchain technology has purportedly seen unregulated crypto investment worth billions of dollars. At least in the US, regulators are closely examining DeFi platforms; for more, see our briefing **As DeFi Matures, US Financial Regulatory Questions Loom Large**.
- There is a renewed focus on the payments sector and its regulation in light of COVID-19's impact on spending habits, and the Wirecard scandal. Payment services firms' prudential risk management and safeguarding arrangements in the event of insolvency are a supervisory priority.
- Greater automation including digitalisation of customer experiences and increased use of third-party providers make firms susceptible to technology disruption events. Ensuring operational resilience remains a regulatory focus whether by way of increasing formal guidance or enforcement action.

- Data use by financial institutions and tech companies, including in AI and algorithmic decision-making, will continue to face scrutiny from regulators. There will also be an increased antitrust enforcement focus on businesses using AI and data.
- In Singapore, the MAS has announced its plans for the development of Project Greenprint, a technology and data platform to support the green finance ecosystem. Four platforms are to be developed. First, a Common Disclosure Portal will allow FIs and corporates to make reliable and comparable ESG disclosures. The project has started with a pilot for listed issuers. Secondly, a Data Orchestrator will aggregate ESG data from different sectoral platforms and trusted data sources. Thirdly, an ESG Registry records and maintains ESG certifications on a distributed ledger, which was launched in May 2022. Lastly, a Greenprint Marketplace will connect green technology providers with investors and corporates and is expected to be launched in 2023.
- While common cross-border standards and regulatory policies with open capital, talent and data flows are unlikely in the short term, some co-operation agreements signed between individual countries have emerged. We expect this approach will continue, with further co-operative mechanisms and countries adopting policies which have been successfully implemented and tested elsewhere.

ARTIFICAL INTELLIGENCE AND THE INTERNET OF THINGS

12. ARTIFICAL INTELLIGENCE AND THE INTERNET OF THINGS

AI

The phrase "artificial intelligence" (AI) presents a challenge to those responsible for coming up with structures and devices to protect hard-won intellectual property. The datasets used to train the AI, so that the system can continuously improve, would probably be protectable as databases. The protection of the AI itself may be by way of copyright in the codes or patents employed. This raises some interesting and complex legal issues for which there are no easy answers.

The copyright law of many countries provides that the author of a computer-generated work is deemed to be the person by whom the arrangements necessary for the creation of the work are undertaken. In an AI scenario, the question of who is

the author arises. Is it the operator of the AI tool or is it the original designer? If the operator uses the software in such a way that copying of third-party works becomes inevitable, a court may find that it was the operator who has caused the infringement. If, on the other hand, the designer designed the software such that copying of third-party works is done routinely, the designer may find it difficult to evade legal responsibility. Liability for infringements by AI systems is likely to be highly fact-specific. This emphasises the need for a mechanism for co-operation between the licensor and licensee in the event a third party alleges that its rights have been infringed by the AI system.

As AI advances, the AI may decide to act autonomously, creating a new work without any particular instructions from the operator or designer to do so. If it is determined there was no human involvement in making the necessary arrangements for the creation of the work, an alleged infringer may raise the unwelcome argument that there can be no copyright in the work since there is no author. It would be difficult to argue that the AI itself is the author, since copyright terms are calculated by reference to the life of the author and are not intended to be indefinite.

Some of these copyright issues may be dealt with in the licence of the AI software between the developer and operator; however, given the enhanced capabilities of AI software, it may be the case that a standard software licence is no longer fit for purpose, particularly where the AI has created the work independently of any human author.

For more, see **Developers can now let an AI assistant write code for them – but what are the IP implications**?

It is also questionable whether any AI-generated work product could be the subject of a patent if the inventors themselves cannot be named. The conclusion reached by a multi-jurisdictional analysis covering various juris dictions in Asia, Europe, the UK and US published by the European Patent Office and Queen Mary University in February 2019 was that the contribution required in order to be considered an inventor must be creative or intelligent in its essence and this requires human intervention. Other than the question of who is the inventor, AI raises fundamental questions in patentability. An invention is only patentable if it involves an inventive step and is not obvious to a

person skilled in the art. A person skilled in the art is deemed to be a skilled technician, aware of the common general knowledge, but lacking imagination or inventiveness. If the inventive step in question can be reduced to the application of an AI system, arguably it will be harder to show that the invention involved an inventive step. Questions raised are whether AI should be deemed to be accessible to the person skilled in the art and, if so, the focus might shift to whether a person skilled in the art would use an AI system in the same way to resolve the problem or otherwise the human intervention involved in the creation of the invention. Patentability will be a bigger issue in fields where inventions arise from the processing of huge amounts of data from considerable investment in experimentation, such as the pharmaceutical industry.

Case law is beginning to emerge on these issues. On 21 September 2021, the English Court of Appeal reiterated that only a human can be considered an inventor for the purposes of UK patent law. For more, see our Talking Tech publication **The Nail in the Coffin for AI Inventorship? – Thaler v Comptroller General**. Dr Thaler is also involved in similar litigation in Australia. On 13 April 2022, the Full Federal Court of Australia likewise held that only a natural person can be an inventor for the purposes of the Patents Act. However, the Australian court stressed that its decision did not mean that an invention by an AI system is not capable of being granted a patent. Since an agreed fact in the case was that Dr Thaler's AI software DABUS was the inventor and not Dr Thaler, the judgment did not deal with the question of whether such a patent application may have a human inventor such as the owner of the machine on which the AI software runs, the developer of the AI software, the owner of the copyright in the AI software source code or the person who inputs the data used by the AI software to develop its output. As such, this question remains undecided.

Other than questions surrounding IP protection, the use of AI also raises legal risks and ethical concerns. Legal risks include:

- Misuse of data: how personal data is used and processed by AI leads to queries as to the logic involved and the consequences of such processing. Potential issues arising from data protection principles are, for example, ensuring that personal data remains accurate, those surrounding any new purpose in the use of the personal data and the consent required, security of personal data including protection against unauthorised or accidental processing, and making available policies and practices in relation to personal data.
- Discrimination: there is an inherent risk of AI incorporating biased datasets and creating biased outcomes, which can lead to unfair or discriminatory decision-making. The use of AI needs to be monitored to avoid potential discrimination claims.
- Anti-competitive conduct: AI may also potentially be used in an anti-competitive manner; for example, the misuse of algorithms to fix prices. In the UK, the Competition and Markets Authority fined an online seller of posters and frames for

using software to implement an agreement with a competitor not to undercut each other's prices.

- Financial misconduct: The potential to lead to financial crime or misconduct is another complication from the use of AI. For example, in its use in trading, firms should ensure datasets do not contain confidential information that amounts to inside information. If algorithms are used to make orders, firms should ensure they do not behave in a manner that constitutes market manipulation, whether immediately or through iterative learning. Where AI is used in generating published or disseminated research or information, firms should check that such information is not misleading.
- Liability in contract and tort. Use of AI by an entity's suppliers or customers may give rise to unintended consequences and may expose entities to contractual or tortious claims. Entities should review their terms and conditions including the boundaries of exclusion clauses.

Ethical issues include transparency and explaining how the technology works; trustworthiness and predictability and making the system auditable and accountable; and fairness and avoiding biases.

Attempts have been made to regulate AI and protect the rights of users. For example, China has promulgated administrative measures regarding algorithm recommendation management in relation to Internet information services, imposing various requirements such as disclosing the basic principles of AI algorithms, providing users with the option of closing algorithm recommendation services, and setting up effective portals for user complaints. The Shenzhen Special Economic Zone has also passed specific rules to regulate AI, as well as to promote the AI industry by laying down an inclusive and prudent supervision framework.

In addition, where the application of existing laws to emerging technologies may not be clear, ethical guidelines may be used to plug regulatory gaps. The Beijing Academy of Artificial Intelligence (BAAI), in collaboration with Peking University, Tsinghua University, Chinese Academy of Sciences, Baidu, Alibaba and Tencent, has issued principles to guide the development and use of AI. This is in the context of a state development plan aiming to make China the world's primary innovation hub by 2030 and an investment promise of US$150 billion to fund AI over the next decade. Hong Kong's Office of the Privacy Commissioner for Personal Data also issued Guidance on the Ethical Development and Use of Artificial Intelligence in August 2021. This outlined seven ethical principles for AI, which not only helps organisations to understand and comply with local privacy law when they develop and use AI, but are also in line with international principles. The seven principles are: accountability; human oversight; transparency and interpretability; data privacy; fairness; AI providing benefits and preventing or minimising harm; and reliability, robustness and security.

In light of the legal risks and ethical concerns, reliance on existing laws and ethical guidelines may not be sufficient and further regulation is inevitable. With AI being a

neutral technology, how we use it and safeguard it is up to us. We need to understand our relationship with it and where society should demand controls on its use.

In November 2021, we published the results of a global study that we commissioned seeking to understand what these safeguards and controls might look like. We found that there is widespread optimism about the potential for AI to transform society and the economy for the better. Whilst policy influencers see AI rules as inevitable, only a third of our respondents are confident in the ability of rule-makers to design and apply suitable rules for artificial intelligence that will have a long-term positive effect. Our aim should therefore be to ensure that AI rules are appropriate and empower people and organisations to pursue noble aims that benefit society. We hope this survey empowers decision-makers to continue their exploration of where their focus needs to go next. Key findings include:

- There is strong support for the application of AI to straightforward, everyday tasks in the private sector (77% support). However, challenging issues that involve judging individuals, such as facial recognition (46% trust), are deeply polarising, with many still not prepared to trust the technology.
- There is a concern that AI will entrench existing inequalities, benefiting bigger businesses (78% positive effect from AI) more than the young (42% positive effect) or those from minority groups (23% positive effect).
- Industry self-regulation is considered a positive step (46% consider effective), but is widely seen as inadequate. That said, the most popular regulatory approach is still sector-by-sector (62% consider effective).
- Few believe that there is a trade-off between robust regulation and innovation (only 31% believe regulation will be so prescriptive that it harms innovation).
- There is a noteworthy degree of willingness for enhanced operational requirements, even if they may prove burdensome for business, including the mandatory notification of users every time they interact with an AI system (82% support).

Please see **A Global Study – Our Relationship with AI: Friend or Foe**.

AI Trends to Watch

Machine learning and artificial intelligence (AI), with the capacity to unlock huge volumes of data, are already being used across a wide range of sectors to cut costs, improve performance and create new processes, services and products. Looking ahead, AI will remain a driver for innovation across sectors, from healthcare and pharmaceuticals, to automobile, and to insurance and financial services. As the transformative potential of AI-enabled technology is being realised in practice, regulatory scrutiny and consumer concern about the legal, ethical and reputational risks of using AI continue to grow.

What's next?

- **Legislation to address the risks posed by AI**: Looking ahead, we expect to see regulation coming to the fore: the European Union's proposed AI regulation is being viewed with interest, given its potential far-reaching scope and influence; US federal regulation is on the horizon, following the introduction of the Algorithmic Justice and Online Platform Transparency Bill in the Senate in 2021, and a recent announcement by the US Federal Trade Commission. We shall also see further laws, guidelines, frameworks and standards targeting specific local jurisdictions, or specific sectors or types of AI-enabled technology, such as autonomous vehicles and facial recognition technology.
- **Responsible AI**: The hidden or unethical use of AI, or failure to tackle the risk of AI bias, could cause severe reputational damage to businesses. Regulatory oversight will also target prudential aspects of "responsible AI" – companies will be expected to have in place documented governance frameworks with clear lines of accountability, robust development, testing and monitoring processes throughout the AI life cycle, and those with oversight responsibilities will be required to have the right expertise. Businesses will also need to understand their reliance on any third-party AI.
- **Litigation risk**: We have already seen court cases on AI explainability brought under data protection laws, and data protection authorities taking action on AI-based facial recognition technology. As legal requirements relating to AI expand and AI use becomes more widespread and potentially more independent of human involvement, questions arise as to development and use standards, liability, rights and ownership in potential copyright works and patentable inventions. IP and commercial disputes relating to AI can be expected in the coming years.

For more, see our publications: Artificial Intelligence in Financial Services – What are the Challenges?; The New EU Regulation on Artificial Intelligence; The Future of AI Regulation in Europe and its Global Impact; Impact of the New EU AI Regulation on Financial Sector Firms – Beware its Extraterritorial Scope; The Italian Courts Lead the Way on Explainable AI – Embracing the Risk-Based Approach Envisaged in the Draft EU AI Regulation; Inclusive Artificial Intelligence: a Legal Perspective – Building Trust Around AI; UK Aims to Become a Global AI Superpower – AI Strategy Published; What is the UK's New AI Playbook?; All Eyes on AI – Australian Government Launches Australia's First AI Action Plan; ICO to Fine Clearview AI £17 million over the Use of its Facial Recognition Tech; and Texas AG Sues Meta (FKA Facebook) Over Biometric Data Collection and Use. See also our contribution to Financier Worldwide: Q&A – Managing AI in the Financial Services Sector.

IoT

The IoT is becoming a reality, enabling connected devices to interact with other devices and to collect and share data on an unprecedented scale. From home thermostats remotely operated using an app on your mobile phone to refrigerators that order groceries, the IoT is focused on making devices "smarter" by integrating embedded computer processors and internet connectivity. IoT does not stop at making white goods more communicative: its applications span the whole spectrum of machine-enabled activities, from retail (automated stock monitoring, point-of-sale analytics), transportation (smart roads and traffic management interacting with connected cars) to health (wearable devices monitored remotely by AI-enabled diagnostic systems), just to name a few.

Two common denominators of IoT technologies are that they involve the collection and transfer of data, which may in many applications (both consumer and industrial) include personal data, and that they automate much of the communication and processing of that data between disparate devices, limiting direct human agency in dealing with that data.

As such, questions arise regarding how privacy and security of the data will be safeguarded. Individual consumers should be entitled to have certainty as to who controls and has access to their information, how it might be used, and, ultimately, who will be liable for misusing the data. The embeddedness in consumers' personal space and the always-on functionality of many IoT devices implies personalised data being processed on a whole new level, all the while subject only to limited individual control. This has triggered concerns about the rise of practices termed "algorithmic discrimination", whereby highly sensitive personal data collected by IoT devices can impact an individual, such as their credit rating, access to health insurance, or the enjoyment of rights and freedoms.

Access to detailed personal data greatly facilitates fraudulent impersonation, which can lead not only to unauthorised access to banking and other sensitive services, but can of itself also be used as a means of gaining access to protected networks by passing off as an insider. A key issue will be to allocate responsibility for security breaches, when the very nature of IoT means a fragmented and diffuse network of devices interoperating and communicating autonomously. The question has to be asked whether existing contractual models of responsibility and liability are sufficient to meet the challenges of the IoT-connected world.

For more on the IoT, please see our Talking Tech webpages

talkingtech.cliffordchance.com

PRODUCT LIABILITY

13. PRODUCT LIABILITY

Product liability actions may be brought in respect of loss or harm caused by product defects associated with manufacture, performance or design, or where an inadequate warning on how to use the product safely has been provided. These claims can arise in respect of both physical and intangible product defects (for example, for defects in both cars and their software).

Product liability claims can be brought in tort, for breach of contract, or for misrepresentation. The most commonly encountered theories of liability are strict liability, negligence, misrepresentation and breach of warranty.

Strict liability:
Even when a manufacturer exercises all possible care in attempting to build safe products, sometimes a product will nonetheless contain an unsafe defect. "Strict" liability imposes liability regardless of whether there has been negligence on the part of the manufacturer, justified by consumer expectations that products should ordinarily be safe to use. Historically, and to a significant extent today, strict liability has been invoked with respect to manufacturing defects, design defects and "*failure to warn*."

Negligence:
Product manufacturers have a duty to exercise a reasonable degree of care in designing their products to be safe and fit for use when used in reasonably foreseeable ways. For example, a software product that assists with the monitoring of safe systems of work, or an AI-based system used in medical diagnosis, should each be designed and delivered to avoid foreseeable risks of harm.

Misrepresentation:
Misrepresentation involves the communication of false or misleading information. Liability for misrepresentation can occur when a person who reasonably relies on that information suffers harm. For example, a software manufacturer that represents that a software product can perform functions which are not within its capabilities, or an EV manufacturer that claims its EV vehicle will charge to capacity in under 15 minutes and maintain battery capacity for two years, can face claims if these representations turn out not to be true.

There are several subcategories of tortious misrepresentation:

- **Fraudulent (also called intentional) misrepresentation**: when a party knowingly provides false or misleading information that causes harm;
- **Negligent representation**: when the party providing the information knew or should have known that it was false; and
- **Strict liability for misrepresentation**: can be asserted without the need to show whether the defendant knew that the information was false.

As noted above, misrepresentation claims are available in respect of intangible products as well as tangible. For example, retail businesses that lose profits due to ongoing malfunctions in payment software may be able to bring a claim based on misrepresentation if the software has been advertised to them as reliable.

Misrepresentation does not always involve a product defect. In the example above, it is possible that the EV is perfectly functional but it takes 30 minutes to charge. The liability then arises not from any manufacturing or design defect, but because misleading information about the vehicle's capabilities has been conveyed to the buyer.

Breach of Warranty:

Warranties are assurances, either explicit or implicit, that goods being sold (or leased) are of sufficient quality and are created through the process of marketing and selling products. If such assurances turn out not to be true, and if an injury to a purchaser occurs as a result, then they may have grounds for a product liability claim based on breach of warranty.

An express warranty can be created and breached through:

- a description of goods provided pursuant to a sale. For example, if an automated parallel parking technology provider describes its system in online marketing brochures as able to "parallel park in spaces only three feet longer than the vehicle", but in fact sells a system that only works in spaces at least five feet longer than the vehicle; or
- a sample employed during the sales process. For example, where a buyer purchases a new vehicle partly based on a demonstration of a manufacturer-installed automated parking system on a vehicle different from that they eventually purchase, and then finds that the system included with their own vehicle does not perform as well as the demonstration model used in the sale.

An **implied** warranty may also be available where goods are sold under an implicit warranty that they are of merchantable quality and fit for the purpose for which they are sold. The Uniform Commercial Code provides a six-part test with respect to merchantability; a less formal definition is "a product of a high enough quality to make it fit for sale".

In addition, a seller of goods creates an implicit warranty that the goods will be fit for the purpose for which they are sold. An automated parallel parking system should be capable of using automation to help a driver park a vehicle. If, instead, the system automatically rotates the steering wheel in a manner that makes it impossible to use without causing a collision, a purchaser of the vehicle can assert that the implied warranty accompanying the sale of the product has been breached.

The potential defendants – a 3D example

One issue that arises in product liability claims is the question of the appropriate defendant, particularly in the age of digital products.

In the example of a 3D-printed medical device, organ or drug, several parties are involved in the production process:

- the owner of the digital design blueprint;
- the 3D printer manufacturer,
- the service or pharmaceutical company; and
- the hospitals and doctors.

Imposing liability on the 3D printer manufacturer is unlikely, unless the alleged injury is caused by a defect in the 3D printer itself. The owner of the digital blueprint is more likely to attract a claim – however, the distribution of liability is less clear.

In the 3D printing scenario, device and drug manufacturers do not "*manufacture*" anything tangible, but are designers and sellers of digital files for others to print medical devices and drugs using their own 3D printers.[19] A finding of strict liability may depend on how courts answer the question of whether a digital file is a "*product*".

An overwhelming majority of jurisdictions currently refuse to apply strict liability principles to claims against hospitals and physicians involving the distribution of allegedly dangerous medical devices or drugs, reasoning that hospitals and physicians provide services rather than products. As 3D-printing becomes more commonplace and hospitals start to incorporate 3D-printing centres, the distinction between providing products and services may become less clear, and the traditional aversion to strict liability may be reconsidered.

19. For examples of 3D printed drugs, see Omnia Ibrahim, Labiotech.eu, Five companies personalising treatments with 3D printed drugs, 28 July 2022, https://www.labiotech.eu/best-biotech/five-companies-personalizing-treatments-with-3d-printed-drugs/

OUTSOURCING

14. OUTSOURCING

As technology increasingly becomes an intrinsic part of any operation or business, outsourcing arrangements are becoming widespread. This may be for cost reasons, but often the outsourcing provider will have greater expertise than that readily available in-house.

Outsourcing may give rise to issues such as where software will be developed; ongoing maintenance and support; the appropriate model for protecting and sharing intellectual property; privacy and data protection concerns; meeting localised regulatory requirements (if any); disaster recovery planning; how liability will be shared and possibly capped; and employment arrangements.

Outsourcing also involves risks such as breach of contract in terms of the quality of services provided, delivery schedules, ownership of employee inventions, cybersecurity risks and data breaches; and risks involved in termination, including trigger events and consequences, such as who has the right to use the IP and software after termination.

Fourth-party risk has also become a concern as companies "right source" and select from or mix platform-as-a-service, multi-sourcing, shared services and low-code/no-code solutions as appropriate. These vendors will often engage their own suppliers – fourth-party vendors – over which the ultimate customer may have limited visibility, control or recourse. Reliance on increasingly complex technology (such as AI), widespread use of platform and cloud-based infrastructure, and ever-increasing regulatory focus on cybersecurity, supply chain governance and digital operational resilience, will make "fourth-party risk" introduced through the extended vendor ecosystem an area of focus for many companies.

Case Study: Hong Kong Regulation of Outsourcing

Hong Kong does not have any law that specifically regulates outsourcing. That said, in regulated industries, primarily the financial services sector, regulators are concerned with outsourcing arrangements that have the potential to impact a business' ability to comply with legal and regulatory requirements and provide adequate services to customers. The key is to engage with the relevant regulator and ensure relevant issues are addressed. Common themes are due diligence of service providers; retention of accountability and control over the outsourced activity; risk management; contingency and exit planning; customer data confidentiality and security; additional risks if overseas outsourcing or further subcontracting is involved; and access to records by regulators.

Non industry-specific guidance has also been issued by the Privacy Commissioner regarding the personal data concerns of outsourcing.

Hong Kong Monetary Authority (HKMA)

The HKMA has issued non-statutory guidelines on outsourcing in its Supervisory Policy Manual with guidance note modules on Outsourcing (SA-2) and General Principles for Technology Risk Management (TM-G-1). The Supervisory Policy Manual sets out both the minimum standards banks are expected to attain in order to satisfy the requirements of the Banking Ordinance, as well as best practice recommendations.

SA-2 requires that banks should, in relation to:

- **Communication with the HKMA**, discuss any plan in advance to begin outsourcing in respect of a banking-related business area or to make changes to or amend the scope of outsourcing of such areas. In relation to outsourcing plans, banks should bear in mind the minimum criteria in order to be authorised by the HKMA pursuant to the Seventh Schedule to the Banking Ordinance (Cap 155), which, among other things, requires banks to have adequate accounting systems and systems of control, and carry on business in a manner that is not detrimental to depositors; they should therefore not enter into or continue outsourcing arrangements that might result in the compromise or weakening of internal control systems or business conduct.
- **The outsourcing agreement**, set out (and regularly review) the type and level of services to be provided by, and the contractual obligations and liabilities of, the service provider.
- **Risk assessment**, regularly conduct comprehensive risk assessment on the outsourcing arrangement.
- **Accountability**, continue to retain ultimate accountability for and control of the outsourced activity.
- Assign staff with appropriate expertise to perform due diligence on service providers before selection and to put in place controls to continuously monitor the performance of the service provider selected, as well as its financial condition and risk profile, and its contingency planning. Reporting procedures

should be established to promptly escalate any problem to the attention of management.

- Understand the implications and make provision for its own contingency planning in the event that an outsourced activity is interrupted due to service provider failure. Alternative service providers or bringing back in-house in an emergency should be considered.
- **Customer data confidentiality**, ensure by way of the outsourcing arrangement, proper safeguards and controls for the protection of customer data confidentiality and integrity, such as providing for the segregation of the bank's customer data from that of the service provider and its other clients; delegation of access to authorised employees of the service provider on a needs only basis; and in the event of termination of the outsourcing arrangement, retrieval or destruction of customer data.
- Notify customers that their data may be outsourced.
- **Outsourced data**, retrieve accurate and timely data from service providers and maintain appropriate records on their own premises available for auditors' and the HKMA's inspection. To facilitate access to data by auditors and the HKMA, the outsourcing agreement should also contain a clause that allows for supervisory inspection or review of operations and controls of the service provider as they relate to the outsourced activity.
- **Overseas outsourcing**, understand the implications for its risk profile including relevant aspects of an overseas country including its legal system, regulatory regime, secrecy laws, and sophistication of technology and infrastructure, as well as the right of overseas authorities to access customers' data. If such access is sought, the HKMA should be notified. The governing law of the outsourcing agreement should preferably be Hong Kong law.

In addition, TM-G-1 requires that banks should, in the outsourcing agreement, provide for software and hardware ownership, and regarding further subcontracting, consider providing expressly that notification and/or approval is required for further subcontracting and that the original service provider remains responsible.

Securities and Futures Commission (SFC)

The SFC has not issued its own general outsourcing guidance, but in February 2005 endorsed the International Organisation of Securities Commissions' (IOSCO) Principles on Outsourcing of Financial Services for Market Intermediaries (Principles). IOSCO updated the Principles in October 2021. The said principles cover seven areas: (i) the due diligence process in selecting (and monitoring) the performance of a service provider; (ii) the contract with the service provider; (iii) protection of proprietary and client information and software, disaster recovery planning, and business continuity; (iv) protection of regulated entity and client confidential information; (v) concentration of outsourcing in terms of issues of dependency of regulated entity and where service providers serve multiple regulated entities in critical services; (vi) access to service provider information, and IT systems, premises

and personnel, relating to outsourced tasks, relevant to contractual compliance or regulatory oversight; and (vii) termination procedures and exit strategies.

External electronic data storage providers

Whilst general guidance has not been issued, in October 2019, the SFC issued a circular to licensed corporations on their use of external electronic data storage providers (EDSPs) such as cloud service providers for the keeping of regulatory records. This was supplemented by the publication of answers to FAQs in December 2020. The prior written approval of the SFC is required for such use, as it is required to approve physical premises where regulatory records must be kept. This is subject to the requirements in the circular being met including (i) the EDSP being staffed by personnel operating in Hong Kong and the regulatory records being stored at a data centre located in Hong Kong, otherwise the EDSP must undertake to provide the regulatory records and assistance as requested by the SFC; (ii) the keeping of a detailed audit trail on access to the regulatory records; and (iii) two Managers-In-Charge of Core Functions (MICs) must be designated to keep the digital keys for access to the regulatory records and to ensure information security. For more, see our **RIFC blog post regarding the SFC circular**.

Outsourcing by Online Distribution and Advisory Platforms

Outsourcing is also referenced in the Guidelines on Online Distribution and Advisory Platforms published in July 2019. This provides that where any function (in relation to online distribution of investment products) is outsourced to an external service provider, the licensed online platform operator should exercise due skill, care and diligence in the selection, appointment and ongoing monitoring of the outsourced service provider to ensure proper performance of the outsourced function. Licensed persons providing robo / digital / automated advice should similarly select and monitor any outsourced service provider including in the development, management or ownership of the algorithms used.

Insurance Authority (IA)

The IA has published guidance in the form of a Guidance Note on Outsourcing (GN14) in September 2012, which is supplemented by a Guideline on Outsourcing (GL14) in June 2017. The IA has also issued Questions and Answers on GL14 answering questions on the type of engagement that would be regarded as outsourcing for the purpose of the guidance. What may be considered as outsourcing for the purpose of the guidance when performed by a service provider includes application and claims processing; policy administration such as premium collection, renewals and customer services; human resources management; marketing and research; information system management; and risk management. On the other hand, sales of insurance policies by agents or brokers and medical examinations (involved in the assessment of insurance claims) are not considered outsourcing. Neither are common business services such as banking, printing and courier.

Prior notification
An authorised insurer should give three months' prior notification to the IA when entering into a new material outsourcing arrangement or significantly varying an existing one. The IA has published a checklist of the information to be submitted to it for entering into an outsourcing arrangement.

Ultimate accountability
An authorised insurer's board of directors and management retain ultimate accountability for all outsourced services.

Similar to the HKMA and IOSCO guidance, the IA guidance discusses the essential issues that an authorised insurer should address when outsourcing its services including in developing an outsourcing policy; developing a framework for assessing the qualitative materiality of the outsourcing arrangement such as its impact on the financial position, business operation, reputation, and ability to maintain adequate internal controls and comply with legal and regulatory requirements; conducting risk assessment; conducting due diligence in the selection of the service provider; negotiating the outsourcing agreement; monitoring and maintaining control of an outsourcing arrangement including where the service provider in turn subcontracts; contingency planning; protecting information confidentiality; and considering the additional risks in overseas outsourcing.

Government outsourcing

A General Guide to Outsourcing was issued in March 2008 to enable the private sector to better understand the procedures and practices followed by government departments
in outsourcing.

Personal data protection

Data processors
The financial regulators in Hong Kong have emphasised the concern of personal data protection, integrity and security in outsourcing. The Office of the Privacy Commissioner for Personal Data (the Privacy Commissioner) has issued guidance in the form of an information leaflet on Outsourcing the Processing of Personal Data to Data Processors. Examples of data processors included in the information leaflet are the engagement of a business services company to administer employee payroll, a marketing company to carry out a customer opinion survey, a service provider to input personal data into a computer system or a contractor to shred documents.

The Privacy Commissioner reminds that a data user must take all reasonably practicable steps to safeguard the security of personal data, retain the same no longer than is necessary for the purpose for which the data is used and obtain consent where it is used for a new purpose. Where data processing is entrusted to a data processor, the data user remains responsible for the acts done by the data processor. Amendments to the Personal Data (Privacy) Ordinance to hold data processors accountable were proposed in January 2020, but no concrete proposals as to the specific wording of the amendments have been published and there is no indication of the intended legislative timetable.

Contractual and non-contractual oversight
The data user must use contractual or other means to monitor its data processor's compliance with data protection requirements. The information leaflet contains examples of the types of obligations that may be imposed on data processors contractually, as well as examples of non-contractual oversight and auditing mechanisms such as selecting reputable data processors which have robust policies in place.

Cloud service providers
Special concerns arise from the engagement of data processors in the form of cloud service providers. The Privacy Commissioner has also issued guidance in the form of an information leaflet on cloud computing (as the SFC has issued guidance on the engagement of EDSPs). The special concerns dealt with in the information leaflet include data centres being distributed across multiple jurisdictions resulting in personal data flowing between jurisdictions, cloud service providers engaging their own subcontractors, cloud service providers only offering services on standard contract terms, and cloud service providers which require the use of their software or the use of shared public clouds.

GAMING

15. GAMING

Video games have been a popular form of entertainment since their creation and have played a key role in shaping pop culture across the world. In recent years, video games have dominated entertainment retail sales, with the global video games market predicted to exceed US$300 billion by 2025.[20]

The explosion in sales is in part due to advances in technology and the accessibility of online gaming, which have allowed for the globalisation of video games on an unprecedented scale. Improved internet speeds, mobile gaming and free-to-play models have made video games accessible to groups of gamers that may not otherwise have had access to a gaming platform.

While the global COVID-19 pandemic has been challenging for many industries, for the gaming industry there are now more developers, content creators and new games coming to the market than ever before, and the new generation of gaming consoles and the advent of 5G mobile connectivity offers new opportunities for stakeholders across the industry. Moreover, reports of increased online purchases and gaming activity in the market coincided with the lockdown measures put in place by governments across the world in response to the COVID-19 pandemic.

With this in mind, we created an all-in-one guide for those that currently operate in or are considering entering the video games industry with the purpose of providing an overview of the life cycle of a video game – from the early stages of development, past the grind of regulatory compliance, through to the final stages of monetising the product. For the guide, see **Level Up: A Guide to the Video Games Industry**.

Abridged insights into key legal and commercial issues that stakeholders regularly face, ranging from ownership of content, licensing of works and enforcing proprietary rights against unscrupulous third parties are set out below.

Creation and Development

Developers will need to have a team of talented specialists with the skills to be able to create game content, including programmers, designers, artists, musicians, writers and actors. The creation and development of certain content might instead be outsourced to other specialised developers or contractors. It will be important for the developer to ensure that all IP and proprietary works subsisting in works developed are properly managed. In particular, developers will want to ensure that underlying agreements contain appropriate provisions ensuring that works created by an employee or contractor are transferred to the developer.

An example of a dispute over copyright ownership is the case of *Emagist Entertainment Ltd v Nether Games (Hong Kong) Ltd* [2022] HKCFI 899. The dispute arose when Emagist found that the defendants had migrated the source code of a profitable online role-playing game "Ninja Saga" to a server under Nether's administrative control, Nether having been incorporated by the defendants. The defendants claimed that they were entitled to do so as they had been business partners and were co-authors of the works in the games. The court ultimately decided that there had not been any partnership,

20. Global Market Insights, Cloud Gaming Market Size Industry Analysis Report, Regional Outlook, Growth Potential, Competitive Market Share & Forecast, 2019-2025

and the defendants were employees who had been enlisted to help in developing the game and bringing in funding. The employer Emagist was the first owner of the copyright in works made in the course of the employees' employment under the Copyright Ordinance (Cap. 528). Emagist was awarded damages for the loss of revenue caused by the migration. This case is a reminder of the need for game developers to put underlying documentation in place to make clear the ownership of copyright.

Other than copyright, there are a number of different IP and proprietary rights that exist to protect different elements of a video game. These protective rights can be used by the proprietor (and potentially its licensees) to prevent infringement, misuse or misappropriation by third parties of the video game (either in part or as a whole). These rights include database rights, trademarks, patents, designs, rights against passing-off, and trade secrets / confidential information

By way of illustration, video game characters are some of the most important IP assets in the industry and can be the unique selling points for games, franchises or even consoles and merchandise. Ensuring characters are adequately protected is essential. There are various ways of protecting a character's name or likeness including copyright, trademarks, passing-off and designs. English case law has been developing to facilitate protection. Copyright may protect a character's image as an original graphic or artistic work. In *Nova Production Limited v Mazooma Games Limited* [2007] EWCA Civ 219, it was established that the graphics of video games may be protected as individual frames. English case law on newspaper headlines further suggests that names may be protectable as literary works under copyright.

AI-generated Content

There is a long history of Artificial Intelligence within video games. At a basic level, when playing against the computer or interacting with Non-Player Characters (NPCs), there is often some AI involved. However, in recent years, AI has been used in games not only to respond to players' actions, but to create new content with algorithms now capable of building endless random levels, worlds and games from predefined parameters. With the increasing use of AI to create video game content, key stakeholders will need to give consideration to the IP rights that might exist in AI-generated content.

Certain issues arise in the context of AI-generated content. Copyright works must be original in order to obtain copyright protection and this requires the exertions of a human author. English copyright law does contain provision for the protection of "computer-generated works", which ascribes authorship to the person who arranged for the work to be created. For instance, if an entire level in a video game was created by AI, there would be a good argument that the programmers who developed the underlying AI code instructed the AI to generate the level. As AI becomes more advanced, it will be increasingly difficult to determine with certainty who made the arrangements necessary for the creation of the resulting work. Is it the programmers of the game, or the programmers of the AI built into the game? In some circumstances, could it be argued that the player themselves made the necessary arrangements? It may ultimately be impossible to identify a human nexus to certain works created by AI; such works may therefore not have an author, and both the ownership and subsistence of copyright in that work will be called into question.

There is ongoing debate by regulators and lawmakers regarding whether copyright law needs to be adapted to take into account AI-generated works, and on what terms. Developers must meanwhile carefully consider how their Terms & Conditions can be used to deal with ownership of AI-generated content by specifying the ownership of IP as between the relevant parties. In addition, as these technologies and the law surrounding them evolve, developers should continue to seek legal advice to ensure their contracts and licences accurately reflect their use of technology and offer adequate protection under copyright law.

User-generated Content

One trend we are witnessing in the video gaming industry is the increasing amount of gameplay-related content being developed and created by players and fans. Developers and publishers encourage users to create and publish User-Generated Content (UGC) to help build a game's brand awareness by using the user's social media connections to reach new viewers and potential customers. Certain games have adopted UGC-based strategies as part of their digital content and have become some of the biggest gaming brands in the world as a result (e.g., Minecraft and Roblox). That said, UGC raises a number of legal and practical issues that key stakeholders in the gaming industry will need to consider.

For example, games that adopt UGC-based strategies in their gameplay are inherently at risk of claims being brought by third parties for IP infringement. In a recent case, Twitch informed streamers across its platform that it had deleted content violating music copyright laws after receiving a wave of DMCA "take-down requests" earlier in the year.[21] From a US and EU law perspective, the US Digital Millennium Copyright Act (DMCA) as well as the EU Copyright Directive control how copyrighted material is used online and contain provisions to protect companies that act as an online platform from third-party IP infringement claims if they take appropriate action in response to a take-down notice and remove the infringing material. Similar protection or a safe harbour to online platforms and service providers is being contemplated in Hong Kong where a consultation to amend the Copyright Ordinance and introduce a Code of Practice took place between November 2021 and February 2022 (an amendment bill was introduced into LegCo, Hong Kong's parliament, in June 2022 and expected to be passed before the end of 2022).

To mitigate the risks of third-party IP infringement claims, companies that work with UGC are making serious investments in how they moderate and control UGC in connection with their games and/or platforms. This includes not only setting up specialist moderation teams in-house, but also contracting with third-party consultants to provide moderation services and ensure that the gaming and digital community are not creating UGC that risks third-party IP infringement. For instance, Twitch's 'Soundtrack by Twitch' tool is part of Twitch's response to its music copyright problem. The tool curates music that is safe to stream worldwide.

Another method to reduce the risk of third-party IP infringement is to restrict the user's freedom of design. For instance, games developer Mythical Games has created a UGC-based game which allows players to create their own characters and the virtual

21. https://www.polygon.com/2020/10/20/21525587/twitch-dmca-takedown-notice-content

world they interact with using the game creation system. However, Mythical Games ensures that it is the creator of all in-game assets that a user can interact with and prevents users from importing, sculpting or designing their own assets. Accordingly, users can only create out of the assets delivered by the developer, which vastly reduces the risk of third-party IP infringement; however, it also runs the risk of disenfranchising players that expect to have greater creative freedom within the game.

Third-party IP and Personality Rights

Incorporating existing and popular third-party brands and trademarks into video games has also become increasingly common. This enables developers to increase game content, advance user experience and benefit from the reputation of the brand to attract new customers. In exchange, third parties can commercialise and monetise their brand by: a) charging the developer a royalty or licence fee; and/or b) using the video game as a platform to advertise its products and services to a wide group of users.

For instance, see our Talking Tech publication Co-Branding Partnerships in the Physical and Digital Worlds – A Masterclass from Balenciaga and Fortnite.

It is also commonplace for sports video games to collaborate with sports retail giants to use their trademark on clothing, merchandise and advertisements in and around the game.

A number of sport celebrities have licensed their personality, name and image rights to developers for use in different sport video games as playable characters (e.g., FIFA, Madden NFL, NBA) and/or to endorse the game concept itself (e.g., Tony Hawk's Pro Skater, Tiger Woods PGA Tour). In certain cases, this will involve the celebrity providing important input on the design and mechanics of the game based on their technical knowledge of the sport. In recent years, we have also seen an increased trend in developers collaborating with celebrities to physically act (using Motion Capture or Performance Capture) and voice act in video games. For instance, Hideo Kojima's blockbuster game "Death Stranding" made use of an enviable cast of actors and actresses to create the game's lead characters, including Norman Reedus, Mads Mikkelsen and Guillermo del Toro.

The existence and scope of personality rights varies between jurisdictions. From a UK perspective, personality rights include:

Name rights: given name, family name, stage name, nickname, etc.

Image rights: facial and body features, distinguishing marks (e.g., birthmarks, tattoos), hair style, distinctive and associated apparel, etc.

Voice rights: sound and likeness of voice, voice recordings, famous catchphrases, etc.

There is no English law that a celebrity has a general right to control the use of their image in all contexts. Instead, a celebrity seeking to control the use of their image may rely upon another cause of action, e.g., passing off, as in the 2015 case of *Rihanna v Arcadia* (concerning a Topshop T-shirt bearing her image); breach of contract; breach

of confidence; infringement of copyright, trade-marks or domain names; defamation; or multiple causes of action simultaneously. Similarly, in Hong Kong, a well-known case concerning the protection of personality rights through passing off and breach of contract is *Lau Tak Wah Andy v Hang Seng Bank Ltd* (unreported, HCA 3968/1999, 29 April 1999). In that case, the bank ran a promotional campaign allowing customers to customise their credit cards with photos of popular Hong Kong entertainers, including Andy Lau. The bank had obtained licences to use the photos from Television Broadcasts Limited (TVB), a television broadcaster in Hong Kong. However, Andy Lau claimed that his likeness had been used without his authorisation and TVB's contractual rights to use the photos were limited. He applied for an interim injunction to prevent further use of his image. The court held that in the context of personality or character merchandising, passing off includes an ingredient of misrepresentation that the personality or character in question had endorsed or licensed the relevant product, or somehow could exercise quality control over it. The court refused the injunction, including for the reason that there was no such misrepresentation in this case as the public would not consider that Andy Lau endorsed the bank's products. In China, personality rights are protected by statute. Under Articles 1012 and 1014 of the Civil Code, an individual has the right to enjoy his or her personal name, and an organisation or individual is prohibited from infringement by interference, usurpation, false representation or other means. Article 1019 provides that infringement of portrait rights by vilification, defacement, forgery by means of information technology or otherwise is prohibited. Article 1024 provides that a civil subject has the right to his or her reputation, and an organisation or individual is prohibited from damaging such reputation by way of insult, libel or other means.

IP Licensing Arrangements

Video games are often a complex patchwork comprising IP rights from many different rights holders. In order to lawfully use a party's IP rights, a valid and legally binding IP licence will need to be in place. This could be a stand-alone licence or it could form part of a wider collaboration, partnership, sponsorship or endorsement arrangement, depending on the context.

Some examples of licensing in for developers include:

- IP assignments contained within employment / contractor contracts for the development of the games;
- Third-party licences, including for music; personality rights and adaption rights for films or books; and
- Game engines.

Some examples of licensing out for developers include:

- Publishing agreements – whilst many companies develop and publish the games within the same structure (e.g., Nintendo), it may be necessary for a developer to work with an external publisher to release the game in international markets;
- End user licence agreement – this governs the relationship between the player and the developer / publisher; and
- Merchandising agreements.

Regardless of whether key stakeholders are licensing in or licensing out IP, they will need to consider carefully a number of factors before entering into any IP licensing arrangement, including: the scope of the licence; whether the licensor's intellectual property will be combined with the licensee's or any third party's intellectual property; how the licensed intellectual property is to be monetised; the requirement for any sublicensing, such as to subcontractors or affiliates; termination rights; and liability and compensation, such as for improper use of intellectual property.

Data Protection and Cybersecurity

All industries, especially those in the digital and consumer sectors (therefore, particularly the gaming sector), are increasingly looking to monetise and derive additional value from data that they are exposed to, whilst managing compliance with emerging global data privacy and cybersecurity legal regimes. A key challenge is that the greater the range and depth of data gathered, the greater the scope and magnitude of data privacy legal obligations and therefore the financial and legal risk if things go wrong.

A current high-water mark in terms of data protection regulation is the European (EU) 2016/679 (General Data Protection Regulation) (GDPR). It broadly applies to all businesses which are based in Europe, as well as those that are selling goods and services to, or monitoring the behaviour of, individuals based in Europe. This extraterritorial scope is clearly relevant for the gaming industry, with global games developers (particularly those based in Asia or the US), that are selling games to a large EU consumer base.

There are many other emerging privacy regimes in key gaming markets which can either be seen to track the GDPR or diverge significantly, including in China, which is causing significant compliance challenges for companies managing a global data business.

In the context of the digital gaming space, personal data may include names, identification numbers, location data, online identifiers (such as usernames / handles), IP addresses and cookie identifiers, meaning that potentially a very broad range of industry data is in-scope.

Emerging privacy regimes are increasingly requiring organisations that are collecting data from users, or being provided with such data from third parties, to be transparent as to the scope of, and the reasons for, data collection.

Whilst data is considered by many to be borderless, across the globe there are increasingly restrictions on international data sharing (particularly with respect to personal data), including in key markets such as China, Japan and Singapore as well as in the EU under the GDPR. This means that developers and other organisations within the gaming sector first have to understand and map how data is being shared between countries, and then consider the necessary compliance steps required to permit such data transfers.

Security breaches are another concern and significant recent examples include: (i) Capcom (2020), the developer of Resident Evil, Street Fighter and Monster Hunter, which was subject to a ransomware attack potentially affecting up to 350,000 people;

and (ii) Wildworks (2020), the developer of Animal Games, affecting up to 46 million records.

Fines can be, and have been, levied by regulators in circumstances where inadequate data security measures have been deployed. There is also a clear risk of reputational and brand damage associated with breaches where the public perception is that businesses have been inappropriate custodians of their customers' data.

As a high number of video game players are minors, extra care needs to be given to ensure that their data is protected and to avoid large fines or other regulatory action. When designing your game, it is important to consider taking steps to ensure that you are in compliance with the most up-to-date guidance or rules from your local data regulator.

Litigation and Dispute Resolution

The significant sums at stake in the global video games market – combined with the complexity of obtaining, exploiting and successfully enforcing the requisite portfolio of rights (whether intellectual property rights, personality rights, contractual rights or others) – make the occurrence of disputes an inevitability. Regulatory issues such as data privacy (discussed above) and competition may also lead to civil litigation and regulatory enforcement.

There are numerous interrelated factors that a prospective claimant or defendant must consider when a potential dispute arises. Accordingly, it is critical to adopt a proactive approach from the outset, engaging with the relevant issues and reflecting on the legal and commercial implications of adopting a particular strategy or approach.

You should immediately seek a comprehensive understanding of the nature of the dispute. This will include identifying the factual matrix, any relevant agreements governing the relationship between the parties (such agreements may include, among other things, governing law clauses, jurisdiction clauses and specified dispute resolution mechanisms), the estimated value of the claim and the legal basis upon which any claim is premised. It will typically be advisable to seek legal advice at this stage, as the legal analysis will necessarily inform strategic decisions and dictate the approach to further engagement with the opposing party or parties.

In the event that the dispute proceeds to litigation, in order to ensure that you are able to fully comply with your disclosure obligations, you should take immediate steps to ensure that any evidence relevant to the dispute which you possess or control is preserved. This may entail contacting those responsible within your organisation for record-keeping and technology to ensure that any routine or other deletion procedures are stopped and/or copies made of any relevant material. If evidence is destroyed, there is a risk that it could constitute a criminal offence, that the court would draw inferences adverse to your interests or, ultimately, that the court could refuse to let you defend the action.

The merits of your case will naturally be a key determinant in establishing whether to proceed to litigation, and you should discuss this in detail with your legal advisers. However, there are a multitude of other interconnected considerations that should also be taken into account during these discussions. These will include (but are not limited to): (a) the duration of the case; (b) the cost of litigation; (c) uncertainty of outcome; and (d) reputational / relationship risks.

It is for these reasons that ADR may be preferable. Even if you think ADR will be unlikely to resolve the dispute, you will nonetheless be expected by the court to have considered ADR. ADR mechanisms include mediation, arbitration, early neutral evaluation and expert determination, among others. Each of these mechanisms has its own idiosyncrasies, advantages and disadvantages. It is advisable to assess carefully the use of ADR within the context of the specifics of the dispute and your strategic / commercial goals.

Above all else, it is essential to ensure that case strategy discussions including as to the manner in which to proceed – whether to litigation, alternative dispute resolution or otherwise – occur with your organisation's commercial goals and priorities at the forefront of everyone's minds. It is therefore recommended that key stakeholders are involved in discussions with your legal advisers from an early stage, as this will help ensure that the strategy adopted maximises the likelihood of achieving the desired result.

HEALTH TECH

16. HEALTH TECH

What will the future of the healthcare sector look like? What will be the key drivers and which market segments are expected to grow? We provide an outlook on the following HealthTech trends:

1. Artificial intelligence and machine learning will become key drivers in healthcare, whilst appropriate and comprehensive regulation might lag.

- AI specific regulation is already on the horizon. The EU is at the regulatory forefront in relation to standalone AI regulation with the proposed AI Act and its extra-territorial effect, which will have an impact on other jurisdictions. This is of relevance to AI and machine learning solutions in the healthcare sector.

- There is the question in the field of AI whether the traditional types of intellectual property (IP) protection are sufficient or even suitable to protect, for example, an AI generated work or invention. We can expect legislative reform in this area to address some of the challenges presented.

2. The market segments of medical robotics, remote treatment solutions and telemedicine will experience further growth.

- Already today, we are advising on highly innovative and globally relevant medical robotics solutions that will, in the future, make it possible to treat patients – and even to perform high-precision surgery – without the physician having to be present at the same site.

- This technology gives rise to many legal questions and challenges such as in the areas of intellectual property rights, privacy and product liability.

3. Health data (including synthetic health data) will become a gamechanger.

- As the collection and processing of health data (as a particularly sensitive category of data) is not only associated with considerable risks and challenges, but also with significant costs (for example, in clinical trial settings), new industries have developed that specialise in the collection and marketing of health data (such as, for example, medical data traders, or companies specialising in research on synthetic health data).

- Synthetic health data (which means representative data artificially scaled on the basis of existing datasets) will become considerably more important – not only for privacy reasons in general, but especially in areas in which the collection of health data is technically or ethically challenging, such as in the case of rare diseases, or with respect to high-risk products, or in the treatment of particularly vulnerable patient groups such as pregnant women or children.

4. Fully integrated virtual healthcare service platforms (together with the health data generated) will become a key focus of health tech development.

- Already today, we are advising on highly innovative platform solutions. These include, for example, fully integrated platform solutions that bring together all market participants in a virtual environment and enable patients to have a consolidated customer journey through all treatment levels and key contacts, from physicians, hospitals or other therapists to pharmacies and health insurers.

- This requires overcoming regulatory issues as well as issues around interoperability of technical systems. We will see more initiatives by industry bodies and governments to bring together standards and policies requiring parties to comply and ensure business continuity.

5. We will see an increase in data incidents and cyber-attacks in the healthcare sector, and data and cybersecurity awareness and safeguards will become increasingly important, as well as appropriate cloud solutions.

- An increase in data incidents and cyberattacks in the healthcare industry is to be expected in the immediate future. One prominent example was the attack on the European Medicines Agency, where even data on BioNTech's COVID vaccine (which was in the approval phase at that time) was allegedly accessed by external hackers.

- In the medium term, data and cybersecurity awareness and safeguards will therefore become an increasingly important ESG compliance issue in the healthcare sector.

CONTACTS

Hong Kong

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Jonathan Wong
Partner
Hong Kong
T: +852 2825 8841
E: jonathan.wong@cliffordchance.com

Jeannie Lam
Senior Associate
Hong Kong
T: +852 2825 8037
E: jeannie.lam@cliffordchance.com

Justin Luo
Registered Foreign Lawyer
Hong Kong
T: +852 2826 3488
E: justin.luo@cliffordchance.com

Jolly Xu
Senior Associate
Hong Kong
T: +852 2826 3404
E: jolly.xu@cliffordchance.com

China

Felicia Cheng
Professional Support Lawyer
Hong Kong
T: +852 2826 3526
E: felicia.cheng@cliffordchance.com

Lei Shi
Partner
Shanghai
T: +852 2826 3547
E: lei.shi@cliffordchance.com

Nathan Zhou
Senior Associate
Shanghai
T: +86 21 2320 7327
E: nathan.zhou@cliffordchance.com

Kimi Liu
Counsel
Shanghai
T: +86 10 6535 2263
E: kimi.liu@cliffordchance.com

Jane Chen
Senior Associate
Beijing
T: +86 10 6535 2216
E: jane.chen@cliffordchance.com

Singapore

Nish Shetty
Partner
Singapore
T: +65 6410 2285
E: nish.shetty@cliffordchance.com

Kabir Singh
Partner
Singapore
T: +65 6410 2273
E: kabir.singh@cliffordchance.com

Janice Goh
Partner,
Cavenagh Law LLP
Singapore
T: +65 6661 2021
E: janice.goh@cliffordchance.com

Joey Ng
Associate
Singapore
T: +65 6661 2059
E: joey.ng@cliffordchance.com

Japan

Natsuko Sugihara
Partner
Tokyo
T: +81 3 6632 6681
E: natsuko.sugihara@cliffordchance.com

Cavenagh Law LLP and Clifford Chance Pte Ltd are registered as a formal law alliance in Singapore under the name Clifford Chance Asia

CONTACTS

Peter Harris
Counsel
Tokyo
T: +81 3 6632 6635
E: peter.harris@cliffordchance.com

Shunsuke Nagae
Senior Associate
Tokyo
T: +81 3 6632 6321
E: shunsuke.nagae@cliffordchance.com

Mohsun Ali
Qualified Lawyer
Tokyo
T: +81 3 6632 6418
E: mohsun.ali@cliffordchance.com

Australia

Naomi Griffin
Partner
Sydney
T: +61 2 8922 8093
E: naomi.griffin@cliffordchance.com

Tim Grave
Partner
Sydney
T: +61 28922 8028
E: tim.grave@cliffordchance.com

Robert Tang
Counsel
Sydney
T: +61 2 8922 8502
E: robert.tang@cliffordchance.com

Haeran Chung
Senior Associate
Sydney
T: +612 8922 8092
E: haeran.chung@cliffordchance.com

Angel Fu
Senior Associate
Sydney
T: +61 2 8922 8089
E: angel.fu@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 27th Floor, Jardine House,
One Connaught Place, Hong Kong

Clifford Chance

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

J2012212-004064